Bezpečnostné aspekty systémov postavených na Open Source

Daniel Olejár
Jaroslav Janáček

20. februára 2004

Obsah

Kapitola 1

Úvod

Súčasná ľudská spoločnosť potrebuje na zabezpečenie svojej existencie a ďalšieho rozvoja spracovávať veľmi veľké množstvá informácie. Preto vytvára a využíva informačné systémy postavené na informačných a komunikačných technológiách (IKT), ktoré umožňujú automatizované spracovanie[1] informácie. Keďže návrat ku klasickému (neautomatizovanému) spracovaniu nie je najmä z kapacitných dôvodov možný, správne fungovanie IKT systémov je nutnou podmienkou[2] úspešného fungovania spoločnosti a jej inštitúcií.

Existuje veľa rozličných faktorov, ktoré môžu ohroziť spoľahlivosť IKT systémov. Preto sa vytvorila informačná bezpečnosť[3] ako disciplína využívajúca poznatky a metódy informatiky, manažmentu, matematiky, práva, psychológie a iných disciplín, na analýzu možných zdrojov ohrozenia IKT systémov a ich informačného obsahu a návrhu opatrení vedúcich k zníženiu vážnosti alebo úplnej eliminácii identifikovaných hrozieb. Jedným z problémov informačnej bezpečnosti je jej multidisciplinárny charakter, druhým jej rýchly rozvoj. To spôsobuje, že použiteľné know-how v informačnej bezpečnosti sa ťažko získava a rýchle zastaráva. Preto je úroveň informačno-bezpečnostného povedomia nedostatočná aj u informatikov, nehovoriac už o laických používateľoch IKT systémov. Úspešné vytváranie a spoľahlivá prevádzka IKT systémov sa bez informačnej bezpečnosti nedá dosiahnuť. Naviac, väčšina opatrení na zabezpečenie IKT systému sa nedá presadiť bez spolupráce laických používateľov týchto systémov. Preto je nutné zvyšovať všeobecnú úroveň poznania informačnej bezpečnosti a adekvátne zohľadňovať jej požiadavky vo všetkých etapách životného cyklu IKT systémov.

Táto práca je čiastkovým výstupom 1. eatapy projektu *Open Source infraštruktúra*, ktorého cieľom je preskúmať možnosti použitia systémov Open Source (v štátnej správe a samospráve). Úlohou tejto práce je preskúmať bezpečnostné aspekty softvérových systémov používaných v IKT systémoch a porovnať z hľadiska bezpečnosti proprietárne

[1] pod spracovaním rozumieme aj zber, prenos, uchovávanie a samotné spracovanie informácie

[2] táto podmienka nie je však postačujúca, spoľahlivo fungujúci IKT systém môže obsahovať nesprávne informácie, resp. ten, kto prijíma rozhodnutia môže podklady z IKT nesprávne interpretovať, alebo ignorovať

[3] informačná bezpečnosť sa chápe ešte aj ako ideálny stav IKT systému, v ktorom je zaistené jeho spoľahlivé fungovanie a ochrana jeho informačného obsahu

a open source systémy. Práca je zatiaľ rozdelená do 3 základných častí.

Aby bolo možné vôbec hovoriť o informačnej bezpečnosti, prvá časť práce poskytuje stručný pohľad na informačnú bezpečnosť. Vychádzajúc z medzinárodného štandardu ISO/IEC 15408, popisujeme všeobecný IKT systém, jeho bezpečnostné ciele, hrozby, ohodnocujeme riziká vyplývajúce z týchto hrozieb, uvádzame bezpečnostné funkcie, ktoré je možné použiť na riešenie zistených bezpečnostných problémov a zaoberáme sa úrovňami bezpečnostných záruk. Táto časť má (laickému) čitateľovi pomôcť vytvoriť si predstavu o predmete a metódach informačnej bezpečnosti.

Druhá časť práce je venovaná základnému softvérovému vybaveniu IKT systémov – operačným systémom a ich bezpečnosti. V tejto kapitole sú analyzované úlohy operačného systému pri zaistení informačnej bezpečnosti IKT systému, popísané bezpečnostné funkcie operačných systémov a z hľadiska bezpečnosti porovnané najbežnejšie operačné systémy.

Ďalšie časti práce budú spracované v druhej etape projektu a budú venované bezpečnostným aspektom vývoja a prevádzky IKT systémov. V týchto častiach práce sa zohľadnia poznatky o bezpečnostných podmienkach, v ktorých budú IKT systémy v štátnej a verejnej správe nasadzované a z bezpečnostného hľadiska posúdia možnosti použitia proprietárnych a open source systémov v týchto IKT systémoch.

Ako vyplynulo z prvej časti, zaistiť bezpečnosť IKT systému nemožno len vhodným výberom, implementáciou, konfiguráciou a údržbou softvéru. Aj keď sa práca zameriava na bezpečnostné aspekty open source systémov, bude v 2. etape riešenia projektu potrebné aspoň stručne analyzovať,čo všetko by bolo potrebné riešiť, aby nedostatky technického, organizačného, prevádzkového či iného charakteru neohrozili bezpečnosť IKT systému.

Práca bude obsahovať niekoľko príloh s informáciami potrebnými pre riešenie bezpečnostných problémov, resp. posudzovanie bezpečnostných aspektov IKT systémov. V prvej etape bol z dodatkov vypracovaný lepšej čitateľnosti je v stručný výkladový slovník bezpečnostných termínov, ktorý má umožniť lepšiu orientáciu čitateľa v problematike informačnej bezpečnosti.

Časť I

Informačná bezpečnosť

Kapitola 2

Základné pojmy informačnej bezpečnosti

V tejto kapitole zavedieme a vysvetlíme základné pojmy informačnej bezpečnosti. Budeme uvažovať abstraktný IKT systém. Tento systém sa skladá z technických komponentov (počítače, periférne zariadenia, komunikačné linky), programového vybavenia (operačné systémy, databázové systémy, aplikačný softvér), údajov (dáta a dokumentácia). IKT systém je umiestnený v nejakých priestoroch (budovy, miestnosti), využíva technickú a komunikačnú infraštruktúru (zdroj elektrického prúdu, klimatizácia, osvetlenie, intranet, Internet, telefónne linky), riadi sa nejakými pravidlami (napr. zákon o ochrane osobných údajov, ochrane utajovaných skutočnostím elektronickom podpise; vnútornou legislatívou organizácie, technickými normami, prevádzkovým poriadkom a pod.) jeho prevádzku zabezpečuje obslužný personál a pracujú s ním používateľia.

Aby sa pri ochrane IKT systému na niečo podstatné nezabudlo, je potrebné daný IKT systém najprv dostatočne podrobne a výstižne popísať. Popis IKT systému sa skladá z popisu samotného IKT systému a jeho bezpečnostného okolia.

Kedže súčasné IKT systémy sú spravidla príliš zložité na to, aby ich bolo možné popísať do detailov, je pri popise systému potrebné uplatniť istú abstrakciu, ktorá umožní túto zložitosť redukovať, pri súčasnom zachovaní tých informácií o IKT systéme, ktoré sú relevantné z bezpečnostného hľadiska. Ukážeme, ako sa vytvára popis IKT systému. Budeme pri tom vychádzať z medzinárodného štandardu ISO/IEC 15408 [4, 6, 3, 5] a metodiky na ňom založenej [2, 7], ako aj z metodických materiálov NIST [1, 14, 12] a [9]. Výsledkom popisu bude *všeobecný bezpečnostný model IKT systému*, ktorý síce nepopisuje žiaden konkrétny IKT systém ale predstavuje akúsi šablónu, ktorú je možno pri popise konkrétnych IKT systémov použiť. Popísaný bezpečnostný model IKT systému sa približuje k tzv. *protection profile IKT systému,* zavedenému v [4]. Popis IKT systému je prvým krokom na zaistenie jeho adekvátnej ochrany a pri jeho tvorbe je potrebné zohľadňovať tri základné otázky:

1. Čo chrániť?
2. Pred čím chrániť?

3. Ako chrániť?

To znamená, že bude potrebné popísať systém, identifikovať nežiadúce možné vplyvy na tento systém a navrhnúť spôsoby, ako tieto vplyvy eliminovať. V ďalšom sa týmito základnými otázkami budeme zaoberať podrobnejšie. Najprv však zavedieme niektoré základné pojmy.

Informačným a komunikačným systémom (IKT systémom) budeme rozumieť súhrn technických a programových prostriedkov, ktoré sa využívajú na prenos, spracovanie alebo ukladanie informácií. Časti IKT systému (subsystémy, technické komponenty, programové vybavenie, údaje,...), ktoré je potrebné z bezpečnostného hľadiska rozlišovať ako samostatné entity, budeme nazývať *položkami (assets)* IKT systému. Pre IKT systém existujú nejaké pravidlá (písané a nepísané) ktoré upravujú jeho činnosť. Akákoľvek udalosť, ktorá môže viesť k odchýlke od týchto pravidiel sa nazýva *hrozbou*. Hrozba je potenciálna odchýlka, ktorá existuje nezávisle od IKT systému. Ak nastane situácia, v ktorej sa hrozba uskutoční, hovoríme o *naplnení hrozby*. Hrozby bývajú orientované na *položky systému*. Napríklad hrozbou je možná krádež počítača, alebo možný prienik do databázy citlivých údajov. Hrozba má svojho nositeľa, entitu (niekoho alebo niečo), ktorá je schopná hrozbu uskutocniť. *Nositeľmi hrozby* môžu byť technické prostriedky, ľudia, ale aj prírodné vplyvy (napr. blesk, záplava a pod.). Hrozby sa môžu realizovať v dôsledku vedomej činnosti ľudí (aj pomocou technických alebo logických prostriedkov), alebo nevedomky, bez úmyslu (ľudský omyl, technická chyba, porucha, prírodný vplyv). Naplnenie hrozby sa nazýva *bezpečnostný incident.* Pokus o vedomé uskutočnenie hrozby sa nazýva *útok*. Ten, kto útok uskutočňuje, sa nazýva *útočníkom*. Na uskutočnenie hrozby je potrebné splnenie nejakých podmienok (napríklad získanie prístupu k systému, vedomosti o systéme, čas, motivácia a pod.). Vlastnosť, technické riešenie, nedostatok systému alebo jeho položky, ktoré úmožňujú realizáciu hrozby, sa nazývajú *zraniteľnosťami* alebo *slabinami systému*. Podmienky potrebné na úspešný útok na systém sa nazývajú *útočným potenciálom*. Uskutočnenie hrozby má spravidla nejaké dôsledky pre systém (strata alebo obmedzenie funkčnosti, finančná ujma). Druhým dôležitým kvantitatívnym parametrom hrozby je pravdepodobnosť toho, že hrozba nastane (že sa naplnia podmienky jej uskutočnenia). *(Bezpečnostné) riziko* vyplývajúce z hrozby je odvodené od pravdepodobnosti naplnenia hrozby a dôsledkov hrozby (vyjadruje sa ako stredná hodnota dopadu hrozby; t.j. ako súčin pravdepodobnosti hrozby a dôsledkov hrozby vyjadrených finančnou stratou, ktorú organizácia naplnením hrozby utrpí). Aktivity alebo prostriedky smerujúce k eliminácii rizík v IKT systéme, alebo aspoň ich zníženiu na únosnú mieru sa nazývajú *bezpečnostné opatrenia.* Cieľom ochrany IKT systému je zabezpečiť jeho bezproblémové fungovanie, t.j. vylúčiť výskyt bezpečnostných incidentov alebo aspoň znížiť bezpečnostné riziká voči systému. To znamená, že pri popise systému je potrebné identifikovať hrozby voči jeho jednotlivým položkám, vyčísliť ich závažnosť (odhad alebo analýza rizík) a navrhnúť a zaviesť bezpečnostné opatrenia. *Bezpečnostná politika (systému/produktu/funkcie)* je súbor pravidiel, ktoré určujú, ako sú položky spravované a chránené. *Model bezpečnostnej politiky* je štruktúrovaná reprezentácia bezpečnostnej politiky. *Bezpečnostná funkcia* systému/produktu je časť systému/produktu, ktorá zabezpečuje dodržiavanie niektorej časti bezpečnostnej politiky. *Bezpečnostný mechanizmus* je konkrétny prostriedok (algoritmus, obvod) realizujúci bezpečnostnú funkciu. *Bezpečný stav systému/produktu* je stav, v ktorom žiadny sub-

jekt nemôže vykonať žiadnu operáciu v rozpore s bezpečnostnou politikou. *Skrytý kanál* je prostriedok, ktorý nie je určený na prenos informácie, no ktorý umožňuje prenos informácie v rozpore s bezpečnostnou politikou. *Manažment konfigurácií* je spôsob riadenia zmien častí systému/produktu počas jeho vývoja a údržby. *Bezpečnostná záruka* je miera dôvery v to, že systém/produkt adekvátne spĺňa bezpečnostné požiadavky. *Neformálny* znamená vyjadrený v prirodzenom jazyku. *Semiformálny* znamená vyjadrený v jazyku s neformálne definovanou obmedzenou syntaxou (napr. rôzne grafické jazyky používané v softvérovom inžinierstve). *Formálny* znamená vyjadrený v presnom jazyku založenom na dobre definovaných matematických princípoch. Viaceré bezpečnostné funkcie IKT systému sú realizované pomocou kryptografických (šifrovacích) funkcií. *Šifrovanie* je proces transformácie informácie $p \in P$ pomocou šifrovacej funkcie $E : P \times K_e \to C$ s použitím šifrovacieho kľúča $k_e \in K_e$ na šifrový text $c = E(p, k_e)$, pričom platí $D(c, k_d) = p$, kde $D : C \times K_d \to P$ je príslušná dešifrovacia funkcia k E a $k_d \in K_d$ je dešifrovací kľúč prislúchajúci k k_e, a bez znalosti k_d nie je p efektívne vypočítateľná[1] z c. Funkcie E a D pritom sú efektívne vypočítateľné. Ak $k_e = k_d$ alebo je k_d efektívne vypočítateľný z k_e, hovoríme o symetrickom šifrovaní (šifrovaní s tajným kľúčom), v opačnom prípade o asymetrickom šifrovaní (vtedy sa šifrovací kľúč k_e nazýva *verejný* a dešifrovací kľúč k_d sa nazýva *súkromný*). V prípade asymetrického šifrovania nesmie byť p efektívne vypočítateľná bez znalosti k_d z c a k_e. *Digitálny podpis* je hodnota $s = S(m, k_s)$ vypočítaná z informácie $m \in M$ použitím podpisovacej funkcie $S : M \times K_s \to C$ s použitím podpisovacieho kľúča $k_s \in K_s$, pričom platí $V(m, s, k_v) = 1$, kde $V : M \times C \times K_v \to \{0, 1\}$ je overovacia funkcia, $k_v \in K_v$ je overovací kľúč, S aj V sú efektívne vypočítateľné, bez znalosti k_s nie je pre dané $m' \in M$ a k_v efektívne vypočítateľná hodnota s' taká, že $V(m', s', k_v) = 1$ a pre dané $m, s = S(m, k_s)$ a k_v nie je efektívne vypočítateľná hodnota m' taká, že $V(m', s, k_v) = 1$.

2.1 Základné aspekty ochrany informácií

Aj keď sme doteraz hovorili o bezpečnosti IKT systémov, treba zdôrazniť, že podstatná je ochrana ich informačného obsahu, t.j. informácie, ktorá sa v nich spracováva, uchováva, alebo prenáša. Pre rôzne typy informácií existujú rôzne požiadavky na ich ochranu. Niektoré informácie je potrebné chrániť pred ich získaním neoprávneným subjektom, iné môžu byť verejné, ale je potrebné chrániť ich pred neoprávnenou modifikáciou. Nedostupnosť informácií pre oprávnený subjekt vtedy, keď ich potrebuje, môže tiež predstavovať vážnu hrozbu. Jednotlivé aspekty ochrany informácií sa navzájom ovplyvňujú a predstavujú určité obmedzenia na prostriedky ochrany. Napríklad ak je určité informácie potrebné chrániť pred prístupom neoprávneného subjektu, ale nie je dôležitá dostupnosť týchto informácií, tak ich môžeme uložiť napríklad v izolovanom počítači uloženom v dobre fyzicky chránenom trezore. Riziko úniku informácií v takomto prípade je určite menšie, ako keď sú informácie uložené v počítači, ktorý je priamo dostupný z Internetu, poskytuje rôzne sieťové služby a umožňuje aj vzdialený prístup k chráneným informáciam. Na druhej strane je dostupnosť informácií komplikovaná potrebou fyzického prístupu. V praxi sa zvyčajne stretávame s kombinovanými požia-

[1] Pod pojmom *efektívne vypočítateľný* sa v tejto súvislosti rozumie známym deterministickým algoritmom polynomiálnej zložitosti.

davkami na ochranu informácií, preto pri hľadaní vhodného riešenia je potrebné nájsť rozumný kompromis medzi rôznymi požiadavkami.

Základné aspekty ochrany informácií môžeme rozdeliť do niekoľkých kategórií:

- dôvernosť (confidentiality),
- integrita (integrity),
- dostupnosť (availability),
- autentickosť (authenticity),
- účtovateľnosť – priraditeľnosť udalostí subjektu (accountability),
- ochrana súkromia (privacy).

2.1.1 Dôvernosť

V informačných systémoch sa často uchovávajú a spracovávajú informácie, ktoré sú dôverného[2] charakteru, t.j. informácie, ktoré majú byť z informačného systému schopné získať len oprávnené subjekty. Cieľom ochrany dôvernosti je zabezpečiť, aby dôverné informácie nemohol získať neoprávnený subjekt. Ochrana dôvernosti zahŕňa ochranu dôvernosti uložených informácií ako aj informácií počas prenosu (napr. počítačovou sieťou). Dôvernosť uložených informácií sa dá chrániť dvoma základnými spôsobmi – riadením prístupu a šifrovaním. Riadenie prístupu môže ochrániť dôvernosť informácií len proti neoprávnenému prístupu prostriedkami systému, ktorý riadenie prístupu implementuje, šifrovanie môže ochrániť dôvernosť uložených alebo prenášaných informácií aj proti prístupu inými prostriedkami (napr. priamy prístup k pamäťovému médiu, na ktorom sú uložené dôverné informácie, odpočúvanie komunikačných liniek).

2.1.2 Integrita

Následkom technických chýb, rušivých vplyvov prostredia, ale napr. aj úmyselnej činnosti útočníkov môže dôjsť k neoprávnenej alebo neúmyselnej zmene uložených alebo prenášaných informácií. Cieľom ochrany integrity je zamedziť takejto zmene alebo umožniť dostatočne spoľahlivo zistiť, že k nežiadúcej zmene došlo. Jedným z prostriedkov ochrany integrity je riadenie prístupu, ktoré môže brániť neoprávneným zmenám informácií prostriedkami systému, ktorý riadenie prístupu implementuje. Vo všeobecnosti však nie je možné zabrániť nežiadúcej modifikácii informácií následkom technických chýb alebo vplyvu prostredia. Taktiež často potrebujeme chrániť integritu informácií aj proti manipulácii obchádzajúcej prostriedky systému alebo integritu informácií prenášaných komunikačnými kanálmi mimo systému. V týchto prípadoch je možné použiť známe techniky umožňujúce zistiť, že informácia bola zmenená. Sú to predovšetkým hašovacie funkcie, hašovacie funkcie s tajným kľúčom a digitálne podpisy. Pomocou hašovacej

[2]Na tomto mieste sa nebudeme zaoberať viacstupňovou klasifikáciou dôvernosti informácií, postačí nám rozlišovať medzi informáciami verejnými a dôvernými.

funkcie sa z informácie vypočíta hašovacia hodnota, ktorá sa pripojí k informácii alebo sa uloží alebo prenesie nezávisle na nej. Pri kontrole integrity sa opäť vypočíta hašovacia hodnota a porovná sa s uloženou alebo prenesenou hašovacou hodnotou. Ak sa informácia (alebo hašovacia hodnota) nezmenila, musia sa obe hašovacie hodnoty rovnať, ak sa zmenila, s veľkou pravdepodobnosťou sa rovnať nebudú. Ak má byť takáto ochrana integrity účinná proti úmyselnej modifikácii útočníkom, musí byť pôvodná hašovacia hodnota uložená alebo prenesená tak, aby ju útočník nemohol nahradiť hašovacou hodnotou zmenej informácie. Vhodným riešením účinným aj proti úmyselnej modifikácii je použitie hašovacej funkcie s tajným kľúčom alebo digitálneho podpisu.

V súvislosti s ochranou integrity nemožno nespomenúť ešte samoopravné kódy, ktoré umožňujú detekovať a opraviť určitý (malý) počet chybných bitov v prenesenej alebo uloženej informácii. Tiež predstavujú spôsob ochrany integrity pred neúmyselnou modifikáciou informácie následkom technických chýb alebo vplyvu prostredia. Ich výhodou je schopnosť opravovať malé (a časté) chyby, no pri zmene väčšieho rozsahu svoju účinnosť strácajú. Nie sú použiteľné ako ochrana proti úmyselnej modifikácii.

2.1.3 Dostupnosť

Častou a dôležitou požiadavkou na ochranu informácií je požiadavka na dostupnosť. IKT systém musí byť schopný poskytnúť oprávneným subjektom informácie vtedy, keď ich potrebujú. Informácie sa môžu stať nedostupnými napr. následkom úmyselnej činnosti útočníka, následkom technického zlyhania (napr. nefunkčný pevný disk, výpadok komunikačnej infraštruktúry, výpadok napájania) alebo aj následkom živelnej pohromy. Niektoré výpadky dostupnosti môžu byť dočasné (napr. výpadok komunikácie), iné môžu byť trvalé (zničenie médií, kde boli informácie uložené). Súčasťou požiadaviek na dostupnosť môže byť určenie maximálneho času, dokedy musia byť informácie poskytnuté, alebo určenie rozsahu výpadku, ktorý musí byť systém schopný tolerovať bez obmedzenia dostupnosti. Dostupnosť sa zvyčajne zabezpečuje redundanciou zdrojov (alternatívne komunikačné kanály, redundantné diskové polia, záložné prostriedky na spracovanie informácií, ...), zálohovaním a archiváciou údajov.

2.1.4 Autentickosť

Aby bolo možné informácie považovať za záväzné (a na ich základe konať), je potrebné popri ochrane integrity zabezpečiť možnosť spoľahlivého určenia ich pôvodu. Informácia je autentická práve vtedy, ak je nezmenená a pochádza od toho, o kom to predpokladáme. V prípade, že potrebujeme chrániť autentickosť informácie len proti narušeniu prostriedkami informačného systému, ktorý ju spracováva, je možné využiť mechanizmy riadenia prístupu. Systém musí spolu s informáciou uložiť a prezentovať aj spoľahlivo overenú identifikáciu subjektu, ktorý informáciu zadal alebo potvrdil (ďalej pôvodca). Ak má byť subjekt, ktorý na základe takejto informácie koná, schopný preukázať, že konal na základe autentickej informácie, musí navyše systém zabrániť zmene uloženej informácie akýmkoľvek subjektom vrátane jej pôvodcu.

Univerzálnym prostriedkom ochrany autentickosti, ktorý navyše umožňuje overe-

nie autentickosti nezávisle na informačnom systéme, ktorý ju spracováva, je digitálny podpis založený na princípoch asymetrickej kryptografie – pomocou súkromného kľúča pôvodcu (známeho len pôvodcovi) sa k informácii vypočíta digitálny podpis, ktorý sa dá následne overiť pomocou verejného kľúča pôvodcu (známeho overovateľovi). Ak sa zabezpečí väzba medzi identifikáciou pôvodcu a jeho verejným kľúčom, digitálny podpis umožňuje dokázať, že informácia je autentická, pretože digitálny podpis závisí na obsahu informácie a na jeho výpočet je potrebný súkromný kľúč pôvodcu.

2.1.5 Účtovateľnosť

Dôležitou požiadavkou na ochranu informácií je možnosť zistiť, ktorý subjekt vykonal bezpečnostne relevantné činnosti – napr. vložil, zmenil, zmazal alebo čítal určitú informáciu. Ak existuje viac subjektov, ktoré sú oprávnené určité činnosti vykonať, je účtovateľnosť potrebná na určenie zodpovednosti v prípade, že bola vykonaná činnosť v rozpore s pravidlami, ktorých dodržiavanie IKT systém nemôže kontrolovať.

2.1.6 Ochrana súkromia

V IKT systémoch sa spracovávajú aj informácie, ktorých podstata nie je dôverná, ale v spojitosti s osobou, ktorej sa týkajú, dôverné sú. Príkladom sú zdravotné záznamy. Pokiaľ nie je možné zdravotné záznamy spojiť s osobou, ktorej sa týkajú, predstavujú len informáciu typu: „Existuje osoba, ktorá mala takéto zdravotné problémy, použila sa takáto liečba s takýmito výsledkami.“ Takáto informácia nemusí byť považovaná za dôvernú. Ak sa k nej pridá informácia o identite pacienta, už sa dôvernou stane, ak sa ju nerozhodne spraviť verejnou pacient, ktorého sa týka. Takáto informácia preto musí byť chránená spôsobom, ktorý umožní prístup k informácii bez častí predstavujúcich spojenie s konkrétnou osobou širšiemu okruhu subjektov a umožní prístup ku kompletnej informácii len užšiemu okruhu oprávnených subjektov.

2.2 Požiadavky na bezpečnosť IKT systémov

IKT systém, ktorý má chrániť spracovávané alebo uchovávané informácie, musí mať určité *bezpečnostné ciele*. Tieto určujú, aké aspekty ochrany informácií sa vyžadujú. Na dosiahnutie bezpečnostných cieľov slúžia *bezpečnostné funkcie*. Požiadavky určujúce, aké bezpečnostné funkcie má systém realizovať, budeme nazývať *funkčnými bezpečnostnými požiadavkami*. Fakt, že určitý systém poskytuje určité bezpečnostné funkcie, však ešte nie je postačujúcim pre vloženie dôvery v bezpečnosť informácií spracovávaných takýmto systémom. Problém je, že bezpečnostné funkcie nemusia byť dostatočné, môžu byť chybne realizované, a pod. Preto sa na dôveryhodné systémy okrem funkčných bezpečnostných požiadaviek kladú aj požiadavky na *bezpečnostné záruky*. Ich cieľom je poskytnúť dôveru v korektnosť implementácie bezpečnostných funkcií a dôveru v dostatočnosť bezpečnostných funkcií na splnenie bezpečnostných cieľov.

Kapitola 3

Popis IKT systému a jeho bezpečnostného okolia

Pri popise systému je v prvom rade potrebné vymedziť IKT systém; t.j. urciť, čo sa považuje za IKT systém (čo sa bude skúmať detailnejšie a do čoho bude možné prípadne zasahovať) a čo za jeho prostredie (o čom bude potrebné prijať isté predpoklady, ale nebude sa to dať podstatnejšie meniť). Systém možno od ostatného sveta odlíšiť stanovením hraníc systému. Aj keď stanovenie hraníc systému nie je absolútne, možno systém charakterizovať ako súbor prvkov/entít, ktoré

1. spadajú pod rovnaký riadiaci manažment,
2. plnia tú istú funkciu, alebo majú rovnaké poslanie,
3. majú v podstate tie isté operačné charakteristiky a bezpečnostné potreby,
4. fungujú vo všeobecnosti v tom istom operačnom prostredí.

IKT systém nepôsobí vo vákuu, a preto treba popísať aj prostredie v ktorom bude pôsobiť a ktoré na jeho činnosť môže mať významný vplyv. Delenie sveta na systém a na „to všetko ostatné“ je však príliš hrubé. Preto zavedieme jemnejšie delenie. To, čo napomáha IKT systému plniť jeho poslanie (napríklad technická infraštruktúra), alebo má širšiu platnosť aj mimo IKT systému ale vzťahuje sa naň (napr. legislatíva), tvorí *bezpečnostné prostredie IKT systému*. Pod pojmom bezpečnostné prostredie IKT systému budeme rozumieť tak fyzické prostredie systému, ktoré môže nejakým spôsobom ovplyvnovať chod systému, ako aj relevantné zákony, bezpečnostné politiky, pravidlá, zvyklosti, skúsenosti a poznatky, ktoré sú pre existenciu IKT systému relevantné [4]. Popis systému je základom pre pochopenie bezpečnostných požiadaviek, ktoré sú s jeho existenciou spojené. Systém preto popíšeme vymenovaním entít, ktoré obsahuje, vzťahov medzi nimi a činnostami, ktoré v systéme, resp. medzi systémom a jeho prostredím prebiehajú. Aktívne entity systému budeme nazývať *subjektami systému*. Subjekty sú nositeľmi, pôvodcami, realizátormi činností prebiehajúcich v systéme. Subjektami systému môžu byť ľudia, technické komponenty systému (server, pracovná stanica), program a pod. V systéme spravidla existujú aj pasívne entity, ktoré budeme nazývať *objektami*

systému. Typické objekty systému sú napr. údaje a technické zariadenia. Rozdelenie na subjekty a objekty je relatívne. Program modifikujúci údaje možno chápať ako aktívnu entitu, subjekt. Ten istý program môže byť objektom, ktorý iný aktívny subjekt (programátor, operátor, administrátor, používateľ) vytvára, modifikuje, spúšťa. Subjekty pristupujú k objektom a vykonávajú nad nimi, pomocou nich alebo prostredníctvom nich nejaké činnosti (prístup subjektu k objektu, vytváranie a modifikácia údajov, spúšťanie programov, prehľadávanie databázy, nastavovanie parametrov technického zariadenia a pod.) Popis systému by mal obsahovať možné činnosti prebiehajúce v systéme. Nie všetky činnosti v systéme sú oprávnené. Štvrtú časť popisu systému tvorí vymenovanie vzťahov medzi subjektami a objektami v systéme. Vzťahy popisujú, aké oprávnenia majú jednotlivé subjekty k objektom v systéme, t.j. či k nim môžu pristupovať a aké činnosti s nimi môžu (legálne) vykonávať. Špeciálnu kategóriu vzťahov tvoria vzťahy medzi subjektami, ktoré však spravidla bývajú stanovené organizačnými dokumentami (napr. prevádzkový poriadok) systému. Popíšeme teraz podrobnejšie, čo je potrebné zahrnúť do popisu systému a jeho bezpečnostného prostredia, aby tieto popisy mohli slúžiť ako základ pre stanovenie bezpečnostných cieľov systému.

Popis bezpečnostného prostredia systému musí obsahovať všetky bezpečnostné aspekty prostredia v ktorom sa systém má používat/používa a spôsob, akým sa používa, resp. plánuje používať. Bezpečnostné prostredie systému charakterizujú

1. Bezpečnostné predpoklady o prevádzke/používaní systému
2. Hrozby voči systému
3. Bezpečnostné organizačné pravidlá

3.1 Bezpečnostné predpoklady o prevádzke systému

Tieto predpoklady explicitne vyjadrujú tie podmienky, za ktorých sa systém prevádzkuje a ktoré sú z bezpečnostného hladiska relevantné. Predpoklady o prevádzke systému možno rozdeliť na nasledujúce kategórie:

3.1.1 Personálne predpoklady

Personálne predpoklady vyjadrujú predpoklady o osobách, ktoré majú prístup k systému (vrátane neoprávnených osôb). Zahŕňa rozdelenie rôl v systéme, kvalifikáciu personálu a používateľov, ich vedomosti o systéme a jeho prevádzkovom poriadku, platnej bezpečnostnej politike, dodržiavaní bezpečnostných opatrení zo strany personálu, bezpečnostnom manažmente systému, riešení bezpečnostných incidentov a pod.

Príklady personálnych predpokladov:

- V systéme sú definované roly: administrátor, audítor, operátor a používateľ. Sú definované roly, ktoré sú nezlúčiteľné: napríklad administrátor a audítor, operátor a administrátor, operátor a používateľ.

- V systéme sa uplatňuje *need to know principle*
- Administrátori, audítori a operátori majú dostatočné znalosti o systéme a pravidlách jeho prevádzky.
- V systéme sa používajú metódy autentifikácie.
- V systéme sa o bezpečnostne relevantných udalostiach vytvára záznam auditu. Záznamy auditu kontroluje audítor.
- Oprávnenia pre činnosť v systéme sa pravidelne kontrolujú. Ak dôjde k zmenám pracovného zaradenia, dôjde aj k prehodnoteniu oprávnení príslušnej osoby.
- Administrátori, audítori, operátori a používateľia sú v potrebnom rozsahu okamžite informovaní o aktuálnych hrozbách (napr. hroziaca vírová epidémia).
- V organizácii spravujúcej systém existuje bezpečnostný manažment. Administrátori, audítori, operátori a používateľia vedia čo majú robiť (na koho sa obrátiť) v prípade bezpečnostného incidentu.
- Administrátori, audítori, operátori a používateľia nezneužívajú svoje oprávnenia.
- Používatelia budú na splnenie svojich úloh potrebovať spolupracovať (prístup používateľov s rozličnými oprávneniami k spoločným zdrojom).

3.1.2 Predpoklady o fyzickom prostredí systému

Vyjadrujú predpoklady o fyzickej bezpečnosti systému. Tieto predpoklady sa vzťahujú na budovu, v ktorej je systém umiestnený (ochrana pred poveternostnými vplyvmi, protipožiarna ochrana, prepätie, blesk, záplavy, ...) fungovanie technickej infraštruktúry (voda, plyn, elektrina, kanalizácia, klimatizácia) a pod. Obsahujú tiež predpoklady o fyzickej ochrane jednotlivých položiek systému pred neoprávneným prístupom a neoprávnenou fyzickou modifikáciou.

Príklady predpokladov o fyzickom prostredí systému

- Budova dostatočne chráni systém pred nežiadúcimi poveternostnými vplyvmi.
- Budova je dostatočne chránená pred prírodnými silami (blesk, povodeň,...)
- Budova je vybavená elektronickým signalizačným zariadením pre prípad požiaru.
- Systém je v budove umiestnený tak, že nehrozí jeho poškodenie v prípade havárie kanalizačného potrubia.
- Budovu stráži strážna služba
- Systém je v miestnosti chránenej elektronickým zabezpečovacím zariadením a bezpečnostnými dverami.
- V budove je inštalovaná priemyselná televízia.

- Do miestnosti v ktorej je umiestnený systém, môžu cudzie osoby vstupovať len v sprievode oprávnených osôb.
- Jednotlivé fyzické komponenty systému sú zaplombované.
- Kabeláž počítačovej siete nie je dostupná z nechránených priestorov.
- Systém je napojený na UPS.
- Budova má vlastný generátor prúdu pre prípad výpadku.

3.1.3 Predpoklady o externých systémoch

Zahrna predpoklady o iných IKT systémoch, ktoré sú nevyhnutné preto, aby daný IKT systém bezpečne fungoval. Tieto predpoklady sú relevantné najmä vtedy, ak je systém, pre ktorý sa tvorí bezpečnostný model, subsystémom rozsiahlejšieho systému (napríklad pracovná stanica, server a pod.) Predpoklady o externých systémoch sa vztahujú aj na spojenie daného IK systému s nimi.

- Použitý operačný systém podporuje prijaté bezpečnostné opatrenia (napríklad autentifikáciu používateľov, sepráciu rôl a pod.)
- Firewall možno nakonfigurovať tak, aby bolo možné do systému pristupovať len z vybraných externých adries.
- Existuje spoľahlivý komunikačný kanál spájajúci IKT systém A s IKT systémom B.

3.2 Hrozby voči systému

Popis hrozieb musí obsahovať všetky hrozby voči jednotlivým položkám systému, ktoré si vyžadujú špeciálnu ochranu či už prostriedkami v samotnom systéme, alebo jeho bezpečnostného prostredia. Pripomíname, že nie je možné zaoberať sa všetkými možnými hrozbami vyskytujúcimi sa v bezpečnostnom prostredí systému, ale je potrebné sústrediť sa na tie, ktoré sú relevantné z hladiska bezpečnej prevádzky samotného systému. Hrozby voči systému možno popísať nasledovne:

- Nositeľ hrozby (potenciálny útočník) je charakterizovaný kvalifikáciou, zdrojmi, ktoré má k dispozícii a motiváciou.
- Útok (metóda útoku, zraniteľné miesto, na ktoré útok smeruje, možnosť/príležitosť).
- Položka, ktorá je cieľom útoku.

Existujú rozsiahle katalógy hrozieb, pozri napr. [9]. Pre všeobecný bezpečnostný model nemá zmysel zaoberať sa konkrétnymi hrozbami, a preto na tomto mieste uvádzame len všeobecnejší prehľad relevantných kategórií hrozieb.

3.2.1 Chyby personálu

Chyby a zabúdanie personálu sú dôležitou kategóriou hrozieb pre IKT systémy. Týkajú sa všetkých používateľov IKT systémov – od úradníkov, ktorí zadávajú vstupné údaje alebo konajú na základe informácií, ktoré získajú z IKT systému, až po systémových administrátorov. Chyby môžu spôsobiť celú škálu problémov - zrútenie systému alebo jeho časti (napr. vymazanie alebo zmena systémového súboru), strata následkom konania na základe chybnej informácie (napr. pokus o doručenie zásielky do nesprávneho ciela) alebo zvýšenie rizika vyplývajúceho z inej hrozby (napr. chyba pri konfigurácii systému môže umožniť prístup neoprávnených subjektov). Mnohé chyby personálu je tažké až nemožné vylúčiť len pomocou prostriedkov IT. Dôležitým prostriedkom na znižovanie rizík vyplývajúcich z chýb personálu sú školenia. Na umožnenie nájdenia zdroja chyby – osoby, ktorá sa chyby dopustila, je potrebné, aby IKT systém vyžadoval identifikáciu a autentifikáciu používateľov a vytváral záznamy auditu.

3.2.2 Krádež a podvod

IKT systémy môžu byť často zneužité na spáchanie krádeže alebo podvodu jednak automatizáciou alebo uľahčením klasických metód, ale aj využitím nových spôsobov – založených priamo na využití (zneužití) IKT systémov. Krádeže a podvody môžu byť takto páchané internými pracovníkmi – oprávnenými používateľmi IKT systému aj externými subjektami. Štatistiky ukazujú, že za väčšinu podvodov sú zodpovední práve interní pracovníci. Interní pracovníci sú velkou hrozbou aj vdaka tomu, že majú prístup k systémom (logický a k častiam IKT systému aj fyzický) a majú znalosti o systéme a bezpečnostných opatreniach, ktoré ho chránia. Velkou hrozbou sú aj bývalí pracovníci, ak sa ich možnosti prístupu nezrušili. Okrem možnosti zneužitia IKT systémov na páchanie krádeží a podvodov môže byť aj samotný IKT systém, resp. jeho časti predmetom krádeže. Následkom toho môže dôjsť nielen k priamym škodám na ukradnutom hmotnom majetku, ale aj k stratám údajov alebo narušeniu dôvernosti údajov, čo môže často predstavovať výrazne vyššie škody, ako hodnota samotného ukradnutého hmotného majetku.

3.2.3 Sabotáž

Zamestnanci môžu svoje znalosti o IKT systéme a jeho zabezpečení, ako aj svoje možnosti prístupu k IKT systému zneužiť na činnosť, ktorej cieľom je poškodiť zamestnávateľa – prevádzkovateľa IKT systému. Motiváciou k takýmto činom je často nespokojnosť zamestnancov so zamestnávateľom (napr. prepustenie zo zamestnania, nespokojnosť v mzdových otázkach a pod.) a túžba po pomste. Táto kategória hrozieb sa týka aj bývalých zamestnancov, ktorým nebol dôsledne zamedzený prístup k IKT systémom po prepustení. Tento typ hrozieb sa napĺňa menej často ako napr. krádeže a podvody, ale často spôsobuje veľké škody.

3.2.4 Strata a poškodenie infraštruktúry

Táto kategória hrozieb zahŕňa najmä požiar, povodeň, vytopenie, explóziu, zrútenie budovy, výpadok dodávavok energií a surovín (elektrina, voda, plyn), prerušenie komunikácie, technické zlyhanie IKT systému, verejné nepokoje, dopravné problémy – neschopnosť zamestnancov dostať sa na pracovisko.

3.2.5 Zlomyseľní hackeri

Zlomyseľnými hackermi sú osoby alebo skupiny osôb, ktoré sa snažia získať určitý stupeň kontroly nad IKT systémom bez povolenia. Ich cieľom býva často osobný prospech – či už získaný priamo napr. zmenou nejakých údajov v IKT systéme alebo ako odmena za získanie dôverných informácií alebo poškodenie informácií v IKT systéme, ale niekedy je cieľom aj len demonštrácia svojich schopností alebo nedostatkov v ochrane IKT systémov, pri ktorej dôjde k stratám. Hackeri môžu útočiť na systémy zvonku, ale často aj zvnútra – či už priamo ako zamestnanci alebo využitím zamestnancov. Útoky zvnútra sú zvyčajne efektívnejšie, pretože mnohé IKT systémy sú výrazne lepšie chránené proti útokom zvonku.

3.2.6 Priemyselná špionáž

Priemyselnou špionážou rozumieme činnosť konkurencie, ktorej cieľom je získať dôverné informácie za účelom zlepšenia svojej konkurenčnej pozície. Z pohľadu bezpečnosti IKT systémov sa priemyselná špionáž môže realizovať využitím hackerov alebo využitím oprávnených používateľov IKT systému, ktorí napr. predajú konkurencii informácie, ku ktorým majú prístup. Priamo zabrániť oprávneným používateľom predávať informácie, ku ktorým majú prístup nie je vo všeobecnosti možné len pomocou prostriedkov IKT systému. Je vhodné, aby zamestnanci mali prístup len k tým informáciam, ktoré potrebujú, a aby sa obmedzovali možnosti ich vynášania mimo IKT systému, ak to nie je potrebné. Účinnou formou ochrany je aj možnosť dokázať, kto k akým informáciam pristupoval, čo si opäť vyžaduje, aby IKT systém vytváral a chránil záznamy auditu.

3.2.7 Zlomyseľné programy

Zlomyseľné programy predstavujú významnú kategóriu hrozieb zahŕňajúcu počítačové vírusy, červy, trójske kone a iné typy nežiadúcich programov. Tieto sa do IKT systému môžu dostať vďaka chybám v častiach IKT systému (operačný systém, aplikačné programy), ale častejšie vďaka správaniu používateľov - prinášanie programov (vrátane dokumentov obsahujúcich makrá) na prenosných médiach (diskety, CD), prezeranie nebezpečných WWW stránok, nebezpečné prílohy elektronickej pošty. Zlomyselné programy môžu spôsobiť priame škody – zničenie alebo poškodenie integrity údajov alebo narušenie ich dôvernosti, alebo môžu zvýšiť riziká vyplývajúce z iných hrozieb (umožnenie prístupu neoprávnenému subjektu).

3.2.8 Organizačné nedostatky

Táto kategória predstavuje hrozby vyplývajúce z chýbajúcich alebo nedodržiavaných organizačných pravidiel (napr. prístup do chránených miestností, pravidlá pre prístup k informáciam a iných položkám, informovanosť pracovníkov o ich povinnostiach súvisiacich s bezpečnosťou), z chybného alebo chýbajúceho plánovania a ďalších organizačných problémov.

3.2.9 Požiadavky vyplývajúce zo záväzných dokumentov

IKT systém bude pôsobiť v prostredí, na ktoré sa vzťahujú všobecne záväzné normy (zákony, vyhlášky), vnútorná legislatíva organizácie, vrátane (ak ju organizácia má vypracovanú) bezpečnostnej politiky. Tieto dokumenty, ktoré budeme nazývať záväznými dokumentami, môžu obsahovať ustanovenia, z ktorých vyplývajú bezpečnostné požiadavky na IKT systém. Všetky bezpečnostne relevantné požiadavky na IKT systém, ktoré vyplývajú zo záväzných dokumentov organizácie treba uviesť v takej forme, aby bolo možné formulovať bezpečnostné ciele. Príklady:

- Informácia sa môže používať len na to, na čo je určená
- k citlivej informácii môžu mať prístup len oprávnené osoby
- uplatnuje sa *need to know principle* (človek má prístup len k takej informácii, ktorú potrebuje na výkon svojich pracovných povinností).
- Právomoci v systéme musia byť pridelené tak, aby nedochádzalo ku konfliktu záujmov (separácia rôl)
- Dostupnosť informácií (informácie sú dostupné oprávneným používateľom napríklad 24 hodín denne)
- Musí sa zaistiť integrita informačného obsahu
- Dôverná informácia sa bude prenášať verejným sieťami len v šifrovanom tvare.
- Osobné údaje musia byť v systéme chránené v zmysle zákona o ochrane osobných údajov.
- Každý pracovník nesie zodpovednosť za svoje konanie.
- Na bezpečnú inštaláciu a prevádzku systému musia existovať dostatočne podrobné návody.
- Informačná bezpečnosť sa musí zohľadňovať vo všetkých fázach životného cyklu systému
- Každý pracovník je povinný okamžite informovať zodpovedného pracovníka o odhalených hrozbách, slabinách alebo bezpečnostných incidentoch systému.

Kapitola 4

Bezpečnostné ciele IKT systému

Deklarácia bezpečnostných cieľov definuje bezpečnostné ciele pre systém a bezpečnostné prostredie systému. Bezpečnostné ciele by mali zodpovedať deklarovanému zámeru (poslanie, ktoré má systém plniť), pritom by mali byť dostatočnou odpoveďou na identifikované hrozby voči systému a pokrývať požiadavky vyplývajúce zo záväzných dokumentov. Bezpečnostné ciele vyjadrujú, čo sa má dosiahnuť, ale nešpecifikujú, akým spôsobom. (To stanovujú až bezpečnostné požiadavky systému.) Bezpečostné ciele IKT systému je možné rozdeliť do nasledujúcich troch skupín:

1. Bezpečnostné ciele samotného IKT systému
2. Bezpečnostné ciele bezpečnostného prostredia IKT systému
3. Bezpečnostné ciele spoločné pre IKT systém a jeho prostredie

Charakterizujeme obsah prvých dvoch skupín bezpečnostných cieľov. Bezpečnostné ciele spoločné pre IKT systém a jeho prostredie sa neuvádzajú samostatne, ale zaraďujú sa do oboch skupín, pre ktoré sú relevantné (t.j. uvádzajú sa dvakrát - aj v skupine bezpečnostných cieľov samotného IKT systému aj medzi bezpečnostými cieľmi jeho bezpečnostného prostredia.)

4.1 Bezpečnostné ciele samotného IKT systému

Bezpečnostné ciele samotného systému korešpondujú s hrozbami a/alebo požiadavkami vyplývajúcimi zo záväzných dokumentov, ktoré bude riešiť samotný IKT systém. Bezpečnostné ciele samotného systému je možné deliť podľa požadovaných bezpečnostných úrovní (ak systém umožnuje/vyžaduje odstupňovanie bezpečnostných úrovní), alebo podľa toho, na čo sa bezpečnostné ciele vzťahujú; napríklad oprávnení používatelia, systém, externé útoky, resp. iné delenie. Nasledujúci zoznam obsahuje vybrané bezpečnostné ciele IKT systému.

1. Kontrola prístupu k zdrojom systému

- História prístupu. Systém zobrazuje informáciu o najnovších úspešných a neúspešných pokusoch používateľa otvoriť session (reláciu) po tom, ako sa používateľovi podarilo otvoriť session
- Autorizácia. Systém musí zabezpečit, aby prístup k údajom a iným zdrojom systému mali len oprávnené osoby.
- Kontrola prístupu založená na autentifikácii žiadateľa alebo jeho roly.
- Obmedzenie prístupu privilegovaných používateľov k zdrojom systému
- kontrola prístupu privilegovaných používateľov
- Obmedzenie činností pred úspešnou autentifikáciou

2. Audit

   - vytvárajú sa záznamy auditu o bezpečnostne relevantných udalostiach v systéme
   - záznamy auditu obsahujú dátum a čas udalosti, lokalizáciu udalosti a entitu zodpovednú za udalosť
   - auditujú sa neobvyklé činnosti oprávnených používateľov
   - záznamy auditu sú dostatočným podkladom pre stanovenie zodpovednosti za aktivity v systéme
   - vytvorene roly audítora na zaistenie nezávislej kontroly činností v systéme (o. i. spracovávanie záznamov auditu)
   - zabezpečenie dostatočných zdrojov (diskový priestor) na vytváranie záznamov auditu
   - ochrana záznamov auditu

3. Komunikácia

   - Kontrola komunikácie z neznámeho zdroja. Systém umožňuje presmerovať, filtrovať, kontrolovať informácie prichádzajúce z neznámeho zdroja.
   - bezpečný komunikačný kanál medzi subsystémami A a B
   - bezpečný prenos údajov v rámci systému
   - zaistenie jednoznačného určeniu pôvodu údajov (*non-repudiation of origin*)
   - zaistenie nemožnosti popretia prijatia údajov (*non-repudiation of receipt*)
   - dostatočné (kapacita a spoľahlivosť) komunikačné linky s externými systémami, resp. prostredím systému

4. Softvér

   - kontrola dodaného softvéru na chyby a úmyselné slabiny (zadné dvierka)
   - Použitie patch-ov a servis pack-ov na fixovanie chýb softvérového vybavenia
   - Overovanie vykonateľného kódu pred jeho spustením
   - izolácia softvéru z nedôveryhodných zdrojov (ak sa pripúšťa spúšťanie programov neznámeho pôvodu, tak len na izolovanom na tento účel vyhradenom počítači)

5. Integrita systému
   - Systém poskytuje prostriedky na ochranu integrity údajov (vrátane zálohovaných a archivovaných) a programového vybavenia
   - systém umožnuje periodické testovanie integrity systému o systém má prostriedky na detekciu a odstránenie zlomyseľných programov (vírusy)
   - Systém má prostriedky na zaistenie fyzickej integrity systému a jeho komponentov
   - Konfiguračný manažment. Implementácia konfiguračného manažmentu na zabezpečenie toho, aby sa systém udržiaval v požadovanom stave.
6. Ochrana údajov
   - Dôvernosť
     - klasifikácia údajov
     - prísnejšia kontrola prístupu založená na identifikácii a autentifikácii používateľov a kontrole ich oprávnení
     - použitie kryptografických prostriedkov ochrany
     - silné algoritmy a ich správna implementácia
   - integrita
     - prostriedky na zaistenie integrity
     - kontrola integrity
   - dostupnosť
     - dostatočný výkon systému
     - dostatočná kapacita komunikačných liniek
     - adekvátna kontrola prístupu o autentickosť
7. ochrana osobných údajov
   - dostatočná frekvencia zálohovania
   - dostatočná frekvencia archivovania
8. Ochrana špeciálnych údajov
   - spoľahlivé generovanie, uchovávanie, prípadne distribúcia autentifikačných údajov (heslá, PIN-y)
   - manažment kryptografických kľúčov
9. Manažment používateľov
   - Bezpečnostné roly (definovanie, zaraďovanie, prehodnocovanie zaradenia)
   - prideľovanie/odnímanie oprávnení na pôsobenie v systéme
   - udržiavanie používateľských atribútov
10. Reakcie na bezpečnostný incident
    - detekcia bezpečnostnch incidentov (treba špecifikovať ktorých)

- automatická reakcia (spustenie alarmu, zablokovanie prístupu,...)
- upozornenie zodpovednej osoby
- záznam auditu[1]
- podpora odstraňovania následkov

11. Bezpečnostné funkcie systému
    - Adekvátne potrebám a možnostiam
    - Korektne implementované o podporené organizačnými opatreniami
    - primerane udržiavané a chránené o pravidelne prehodnocované
12. Prípadne ďalšie bezpečnostné ciele systému.

4.2 Bezpečnostné ciele bezpečnostného prostredia IKT systému

Bezpečnostné ciele bezpečnostného prostredia systému sú odvodené z hrozieb a/alebo požiadaviek vyplývajúcich zo záväzných dokumentov, ktoré nie je možné v plnom rozsahu riešiť v rámci samotného IKT systému. Bezpečnostné ciele bezpečnostného prostredia systému budeme deliť na dve skupiny: bezpečnostné ciele ktoré bezprostredne súvisia s IKT a tie ostatné (non-IKT). Medzi non-IKT bezpečnostné ciele bezpečnostného prostredia IKT systému patria bezpečnostné ciele organizačného charakteru:

- *Dokumentácia:* všetky osoby pôsobiace v systéme (administrátori, operátori, audítori, používatelia,...) majú k dispozícii potrebnú dokumentáciu, čím sa znižuje pravdepodobnosť omylu, chyby založenej na nevedomosti.
- *Kompetentnosť:* všetky osoby pôsobiace v systéme (administrátori, operátori, audítori, používatelia,...) majú dostatočnú kvalifikáciu na to, aby boli schopné plniť úlohy, ktoré sa im ukladajú (resp. ktoré im z ich pracovného zaradenia vyplývajú).
- *Dodržiavanie platných predpisov pri prevádzke systému.* Všetky osoby pôsobiace v systéme (administrátori, operátori, audítori, používatelia,...) poznajú (a dodržiavajú) prevádzkové predpisy systému.
- *Inštalácia systému:* zodpovedné osoby musia zaistiť, aby bol systém doručený, inštalovaný a prevádzkovaný tak, aby nedochádzalo k narušeniu jeho bezpečnosti.
- *Fyzická ochrana systému:* zodpovedné osoby musia zabezpečiť, aby bol systém chránený proti fyzickému prístupu nepovolaných osôb, neautorizovanej modifikácii svojich komponentov. Fyzická ochrana komunikácie (ochrana komunikačných liniek, zariadení proti fyzickému útoku).

[1] Relevantné v prípade napr. pokusu o prienik hackera do systému, nepoužiteľné napr. pre porušenie prevádzkových pravidiel. Ale aj v prípade bezpečnostných incidentov, ktoré sa nezaznamenávajú automaticky, by bolo užitočné viesť záznamy, na základe ktorých by bolo možné jednak stanoviť zodpovednosť za incident a jednak identifikovať slabé miesto systému a prijať príslušné opatrenia na vylúčenie podobných incidentov v budúcnosti.

- *Autentifikácia osôb pristupujúcich k systému*
- *Manažment autentifikačných prostriedkov* (zmena hesiel, kľúčov, výmena autentifikačných tokenov; prehodnocovanie prístupových práv pri zmene funkcie osoby pôsobiacej v systéme
- *Školenia osôb* pôsobiacich v systéme na tému informačná bezpečnost, ochrana systému pre útokmi.
- Zakotviť (napríklad v pracovných zmluvách) *povinnosť zamestnancov oznamovať bezpečnostne relevantné informácie* zodpovedným osobám.

Bezpečnostné ciele bezpečnostného prostredia systému, ktoré bezprostredne súvisia s IKT:

- Operačný systém poskytuje potrebnú odporu (autentifikácia používateľov, separácia rôl, ochrana prístupu)
- Korektné fungovanie bezpečnostne relevantného použitého hardvéru, softvéru a firmvéru
- Periodické testovanie integrity systému (hardvér aj softvér).

Kapitola 5

Bezpečnostné požiadavky IKT systému

Bezpečnostné ciele IKT systému vyjadrujú predstavu, ako by systém mal fungovať, aby sa eliminovali hrozby, resp. splnili požiadavky vyplývajúce zo záväzných dokumentov. Nehovoria však o tom, akým spôsobom sa majú tieto ciele naplniť. Bezpečnostné požiadavky IKT systému konkretizujú bezpečnostné ciele IKT systému prostredníctvom bezpečnostných funkcionálnych požiadaviek a požiadaviek na bezpečnostné záruky. Bezpečnostné funkcionálne požiadavky predstavujú bezpečnostné funkcie, ktoré by mal IKT systém plniť, aby naplnil stanovené bezpečnostné ciele. Bezpečnostné funkcie systému vyjadrujú, čo systém dokáže spraviť na presadenie stanovených bezpečnostných cieľov, ale nehovoria o úrovni záruk, ktoré systém, resp. jeho bezpečnostné funkcie poskytujú. Požiadavky na bezpečnostné záruky špecifikujú čo je potrebné spraviť, aby bezpečnostné funkcie systému naplnili stanovené ciele. Zároveň umožnujú stanoviť/posúdiť úroveň dôvery v systém. Pre reálny systém (reálne existujúci, alebo taký, o ktorom sa vie, v akých podmienkach bude pôsobiť) je možné eplicitne stanoviť aj bezpečnostné požiadavky na bezpečnostné prostredie systému.

5.1 Funkcionálne bezpečnostné požiadavky

V tejto časti postupne popíšeme jednotlivé triedy funkcionálnych bezpečnostných požiadaviek v súlade so štandardom ISO/IEC 15408 Common Criteria [2] a [3]. Zoznam tried funkcionálnych bezpečnostných požiadaviek predstavuje akýsi katalóg, z ktorého sa budú vyberať opatrenia na realizáciu stanovených bezpečnostných cieľov. Význam tohto katalógu spočíva v jeho úplnosti ; t.j. že na existujúce hrozby voči IKT systému v nom možno nájsť adekvátne protiopatrenia a v konzistentnosti. Common Criteria podrobne popisujú aj závislosti medzi jednotlivými funkcionálnymi bezpečnostnými požiadavkami a požiadavkami na bezpečnostné záruky.

5.1.1 Bezpečnostný audit (FAU)

Bezpečnostný audit zahŕňa rozpoznávanie, zaznamenávanie, ukladanie a analýzu informácií, ktoré majú vzťah k bezpečnostne relevantným činnostiam, t.j. k činnostiam, ktoré sú riadené bezpečnostnou politikou. Záznamy auditu umožňujú určiť, aké bezpečnostne relevantné činnosti sa udiali a kto (aký subjekt) je za na zodpovedný.

Automatické reakcie (FAU_ARP) Táto skupina definuje činnosti, ktoré sa automaticky vykonajú v prípade, keď systém auditu detekuje potenciálne narušenie bezpečnosti. Tieto činnosti môžu zahŕňať širokú škálu – od upozornenia zodpovedného pracovníka až po aktívne zabránenie následnému prehlbovaniu škôd napríklad prerušením spojenia so subjektom, ktorý narušil bezpečnosť alebo zastavením činnosti nejakého subsystému, kým nebudú vykonané opatrenia na uvedenie systému späť do bezpečného stavu.

Tvorba záznamov auditu (FAU_GEN) Táto skupina obsahuje požiadavky na zaznamenávanie výskytov bezpečnostne relevantných udalostí, ktoré sa stanú pod kontrolou bezpečnostných funkcií. Špecifikuje sa úroveň podrobnosti auditu, zoznam typov udalostí, ktoré sa majú auditovať (napr. prihlásenie do systému, prístup k určitému typu informácií alebo ich zmena, ...) a určí sa minimálna množina informácií, ktoré sa majú v záznamoch auditu uvádzať (napr. čo sa stalo, kedy sa to stalo, s čím sa to stalo, kto to spravil). Rozhodne by sa malo zaznamenávať spustenie a ukončenie činnosti auditu. Každý záznam by mal obsahovať minimálne čas udalosti, typ udalosti, identifikáciu subjektu, ktorý udalosť spôsobil a výsledok udalosti.

Analýza bezpečnostného auditu (FAU_SAA) Táto skupina obsahuje požiadavky na automatizovanú analýzu činnosti systému a záznamov auditu s cielom odhaliť potenciálne narušnie bezpečnosti. Takáto analýza sa využíva ako základ systémov na detekciu prienikov alebo ako zdroj informácií pre automatické reakcie (FAU_ARP). Je viac možných úrovní analýzy záznamov auditu. Najjednoduchším spôsobom je kontrola prekročenia určených hraníc (napr. prekročenie maximálneho počtu chybných pokusov o prihlásenie do systému). Zložitejšie systémy môžu vytvárať profily používania systému (napr. bežné príkazy, ktoré daný typ subjektu používa, typy komunikačných spojení, ktoré využíva, rýchlosť písania na klávesnici) a potom kontrolovať odchýlky od týchto profilov, ktoré často znamenajú (potenciálne) narušenie bezpečnosti. Takáto analýza sa môže vykonávať v reálnom čase alebo aj off-line. Dalšie možnosti zahŕňajú heuristickú analýzu schopnú odhaliť postupnosti udalostí typické pre jednoduché alebo aj komplexné útoky.

Prezeranie záznamov auditu (FAU_SAR) Táto skupina definuje požiadavky na nástroje, ktré slúžia na prezeranie záznamov auditu. Poskytuje oprávneným subjektom čítať záznamy auditu vo vhodnej forme a zabranuje neoprávneným subjektom pristupovať k záznamom auditu. Poskytuje nástroje na vyhľadávanie a triedenie záznamov auditu podla zvolených kritérií.

Výber udalostí pre bezpečnostný audit (FAU_SEL) Táto skupina definuje požiadavky na možnosť výberu udalostí, ktoré sa budú zaznamenávať na základe stanovených atribútov (napr. identita subjektu alebo objektu alebo typ udalosti).

Ukladanie záznamov auditu (FAU_STG) Táto skupina definuje požiadavky na bezpečné uchovávanie záznamov auditu. Základnou požiadavkou je ochrana uložených záznamov auditu proti neoprávnenému vymazaniu a zmene. Systém by mal zmene zabrániť alebo ju aspoň detekovať. Definuje sa aj, čo sa má udiať v prípade, keď sa priestor pre ukladanie záznamov auditu zaplní nad určenú hranicu. Na vyššej úrovni sa definuje, čo sa má robiť v prípade, že nie je možné ďalej ukladať záznamy auditu (napr. po zaplnení priestoru alebo v prípade zlyhania záznamových prostriedkov).

5.1.2 Komunikácia (FCO)

Táto trieda požiadaviek obsahuje dve skupiny, ktorých cieľom je bezpečne identifikovať účastníkov komunikácie. Jedna skupina definuje požiadavky na identifikáciu odosielateľa informácie (dôkaz o pôvode), druhá na identifikáciu prijímateľa informácie (dôkaz o prijatí). Tieto skupiny zabezpečujú. že odosielateľ nemôže poprieť odoslanie informácie a prijímateľ nemôže poprieť jej prijatie.

Nepopierateľnosť pôvodu (FCO_NRO) Táto skupina zabezpečuje, že odosielateľ informácie nemôže úspešne poprieť, že poslal nejakú informáciu. Vyžaduje, aby bezpečnostné funkcie systému poskytovali metódu, ktorou prijímateľ informácie môže získať dôkaz o pôvode informácie. Dôkaz o pôvode môže byť potom schopný overiť prijímateľ prípadne aj iné subjekty. Bezpečnostné funkcie musia byť schopné vytvárať dôkazy o pôvode pre zadané typy informácie na základe požiadavky určených subjektov, resp. vždy. Musia dávať do súvisu zvolené atribúty odosielateľa a vybrané časti informácie, ktorej sa dôkaz o pôvode týka.

Nepopierateľnosť prijatia (FCO_NRR) Nepopierateľnosť prijatia zabezpečuje, že prijímateľ informácie nemôže úspešne poprieť prijatie informácie. Táto skupina vyžaduje, aby bezpečnostné funkcie systému poskytovali odosielateľovi informácie metódu, ktorou môže získať dôkaz o doručení (prijatí) informácie. Tento dôkaz môže potom overiť odosielateľ alebo iné subjekty. Bezpečnostné funkcie musia byť schopné vytvárať dôkazy o prijatí pre zadané typy informácie na základe požiadavky určených subjektov, resp. vždy. Musia dávať do súvisu zvolené atribúty prijímateľa a vybrané časti informácie, ktorej sa dôkaz o prijatí týka.

5.1.3 Kryptografické nástroje (FCS)

Bezpečnostné funkcie systému môžu, zvyčajne na dosiahnutie náročnejších bezpečnostných cieľov, využívať kryptografické prostriedky. Využívajú sa napríklad na zabezpeče-

nie vyššej úrovne identifikácie a autentifikácie, na ochranu dôvernosti údajov – šifrovanie, vytváranie dôkazov o pôvode a prijatí informácie, a ďalšie účely.

Manažment kryptografických kľúčov (FCS_CKM) Kryptografické kľúče musia byť vhodne spravované počas celého svojho životného cyklu. Inak je možné vážne narušiť bezpečnosť kryptografických prostriedkov. Napríklad, ak by sa po skončení používania súkromných alebo tajných kľúčov na vytváranie digitálnych podpisov nezabezpečila ich dôsledná likvidácia a bolo by možné, aby sa k nim dostala nepovolaná osoba, táto by mohla spätne falšovať digitálne podpísané dokumenty. Táto skupina preto obsahuje požiadavky na jednotlivé činnosti, ktoré sa s kryptografickými kľúčmi robia počas celého ich životného cyklu - generovanie kľúčov, distribúcia kľúčov, prístup ku kľúčom a likvidácia (ničenie) kľúčov. Uvádzajú sa požiadavky na algoritmy, parametre kľúčov (napr. veľkosť kľúča), postupy pri vytváraní, distribúcií, prístupe a likvidácii kľúčov.

Kryptografické operácie (FCS_COP) Aby kryptografické operácie fungovali správne a bezpečne, je potrebné aby boli vykonávané podľa príslušných algoritmov a s kľúčmi správnych parametrov. Medzi typické kryptografické operácie patria najmä šifrovanie a dešifrovanie dát, vytváranie a overovanie digitálnych podpisov, vytváranie a overovanie informácií na kontrolu integrity (napr. pomocou kryptograficky silných hašovacích funkcií a kryptograficky silných hašovacích funkcií s tajným parametrom), šifrovanie a dešifrovanie kryptografických kľúčov (napr. v hybridných kryptosystémoch, kde sa dáta šifrujú symetrickým tajným kľúčom, ktorý asymetricky šifruje a pripája k správe), protokoly na dohodnutie kľúča.

5.1.4 Ochrana používateľských dát (FDP)

Táto trieda požiadaviek sa špecifikuje požiadavky na bezpečnostné funkcie a politiky týkajúce sa ochrany používateľských dát. Je rozdelená na štyri časti:

1. Politiky bezpečnostných funkcií na ochranu používateľských dát
   - Politika riadenia prístupu (FDP_ACC)
   - Politika riadenia toku informácií (FDP_IFC)

   V rámci týchto skupín sa definujú a pomenujú rôzne politiky bezpečnostných funkcií riadiacich prístup k položkám systému a toku informácií a ich rámec pôsobnosti. Na tieto politiky sa potom odvolávajú požiadavky na bezpečnostné funkcie, ktoré ich dodržiavanie zabezpečujú a kontrolujú.
2. Spôsoby ochrany používateľských dát
   - Funkcie na riadenie prístupu (FDP_ACF)
   - Funkcie na riadenie toku informácií (FDP_IFF)
   - Vnútorné prenosy (FDP_ITT)
   - Ochrana zvyškových informácií (FDP_RIP)

- Rollback (FDP_ROL)
- Integrita uložených dát (FDP_SDI)

3. Off-line ukladanie dát, import a export
   - Autentifikácia dát (FDP_DAU)
   - Export dát mimo rámec pôsobnosti bezpečnostných funkcií (FDP_ETC)
   - Import dát z mimo rámca pôsobnosti bezpečnostných funkcií (FDP_ITC)

   Tieto skupiny požiadaviek sa zaoberajú dôveryhodnosťou dát, ktoré sa prenášajú medzi systémom a inými systémami mimo pôsobnosti bezpečnostných funkcií.

4. Komunikácia medzi dôveryhodnými systémami
   - Dôvernosť používateľských dát pri prenosoch medzi dôveryhodnými systémami (FDP_UCT)
   - Integrita používateľských dát pri prenosoch medzi dôveryhodnými systémami (FDP_UIT)

   Tieto skupiny sa zameriavajú zabezpečenie komunikácie medzi dvoma dôveryhodnými systémami.

Politika riadenia prístupu (FDP_ACC) Táto skupina obsahuje požiadavky na pomenovanie politík riadenia prístupu a definovanie oblastí ich pôsobnosti. Tieto politiky sú potom súčasťou bezpečnostnej politiky systému. Každá politika riadenia prístupu identifikuje subjekty a objekty a činnosti, ktorých sa týka.

Politika riadenia toku informácií (FDP_IFC) Táto skupina obsahuje požiadavky na pomenovanie politík riadenia toku informácií a definovanie oblastí ich pôsobenia. Tieto politiky sú potom súčastou bezpečnostnej politiky systému. Každá politika identifikuje subjekty, informácie a operácie, ktoré umožnujú prenos informácií medzi subjektami, ktorých sa politika týka.

Funkcie na riadenie prístupu (FDP_ACF) Táto skupina požiadaviek špecifikuje funkcie, ktoré realizujú určenú politiku riadenia prístupu. Tieto funkcie realizujú rozhodnutia, či sa požadovaná činnosť daného subjektu s daným objektom povolí na základe určitých bezpečnostných atribútov subjektov a objektov (napr. na základe identity používateľa a prístupových práv k objektu).

Funkcie na riadenie toku informácií (FDP_IFF) Táto skupina požiadaviek špecifikuje funkcie, ktoré realizujú určenú politiku riadenia toku informácií. Tieto sa týkajú dvoch typov toku informácií – bežného priameho toku informácií, ktorý sa riadi určenou politikou, a nepovoleného toku informácií (skrytých kanálov). Toto delenie vyplýva z rôzneho charakteru týchto spôsobov prenosu informácií. Nepovolené informačné toky v tomto zmysle svojou podstatou obchádzajú politiku riadenia toku informácií a vyžadujú

si osobitný prístup na ich znemožnenie alebo aspoň obmedzenie. Funkcie na riadenie toku informácií, ktoré sa týkajú bežného toku informácií rozhodujú o povolení alebo zakázaní toku informácie medzi subjektami na základe určených bezpečnostných atribútov subjektov a informácie. Funkcie na obmedzenie alebo zabránenie nepovoleného toku informácií musia obmedzovať kapacitu skrytých kanálov na určenú hranicu, prípadne až znemožnovať zneužitie skrytých kanálov na nepovolený prenos informácií. Taktiež sa môže požadovať monitorovanie nepovoleného prenosu informácií.

Vnútorné prenosy (FDP_ITT) Táto skupina požiadaviek sa zaoberá ochranou dôvernosti a integrity dát, ktoré sa prenášajú medzi rôznymi časťami systému. Môže sa tiež vyžadovať separácia prenášaných dát podla určených bezpečnostných atribútov (teda využitie rôznych komunikacných kanálov – napr. s rôznym spôsobom ochrany – pre rôzne typy dát).

Ochrana zvyškových informácií (FDP_RIP) Táto skupina požiadaviek sa zaoberá potrebou zabezpečenia toho, aby vymazané údaje nemohli byť opätovne sprístupnené, a aby novo vytvorené objekty neobsahovali informácie, ktoré nemajú byť prístupné. Po logickom vymazaní údajov sa totiž tieto často ešte fyzicky v systéme nachádzajú (napríklad vymazanie súboru alebo záznamu v databáze sa často realizuje len označením priestoru, ktorý zaberal ako voľný, pričom informácie sa neprepíšu).

Rollback (vrátenie systému do predchádzajúceho konzistentného stavu)(FDP_ROL) Táto skupina definuje požiadavky na schopnosť systému odstrániť efekt predchádzajúcej postupnosti operácií (napr. keď sa postupnosť korektne neukončila, alebo sa zistila chyba) a vrátiť sa do predchádzajúceho konzistentného stavu.

Integrita uložených dát (FDP_SDI) Táto skupina obsahuje požiadavky na ochranu integrity používateľských dát v čase, ked sú uložené v pôsobnosti systému (napr. v operačnej pamäti alebo na záznamovom médiu - disk, páska, CD, ...). Požadovať sa môže, okrem kontroly integrity, aj definovanie činností, ktoré má systém vykonať v prípade, že zistí porušenie integrity.

Autentifikácia dát (FDP_DAU) Autentifikácia dát umožnuje entite prijať zodpovednosť za autenticitu dát. Táto skupina poskytuje metódu na poskytnutie záruky za platnosť určitých údajov, ktoré môžu byť potom použité na overenie, že obsah nejakej informácie nebol falšovaný alebo inak zmenený. Vyžaduje sa, aby bezpečnostné funkcie boli schopné vytvoriť dôkaz, ktorý môže byť použitý ako záruka platnosti určených typov informácií a aby bezpečnostné funkcie umožnovali určeným subjektom overiť si platnosť týchto informácií. Navyše sa môže požadovat, aby určené subjekty mohli zistiť identitu používateľa, ktorý vytvoril tento dôkaz - prijal zodpovednosť za autenticitu dát.

Export dát mimo rámec pôsobnosti bezpečnostných funkcií (FDP_ETC) Táto skupina požiadaviek sa zameriava na export používateľských dát zo systému. Určuje

požiadavky na export dát v prípade, ked je možné k dátam priradiť bezpečnostné atribúty a v prípade, ked nie je možné k exportovaným dátam priradiť bezpečnostné atribúty.

Import dát z mimo rámca pôsobnosti bezpečnostných funkcií (FDP_ITC) Táto skupina požiadaviek sa zameriava na import používateľských dát do systému. Používatelské dáta sa môžu importovať bez bezpečnostných atribútov – v tom prípade sa bezpečnostné atribúty určujú zvlášť, alebo sa môžu importovať aj s bezpečnostnými atribútmi, ktoré sa zachovajú.

Dôvernosť používateľských dát pri prenosoch medzi dôveryhodnými systémami (FDP_UCT) Táto skupina definuje požiadavky na zabezpečenie dôvernosti používateľských dát pri prenose medzi dvoma dôveryhodnými systémami.

Integrita používateľských dát pri prenosoch medzi dôveryhodnými systémami (FDP_UIT) Táto skupina definuje požiadavky na zabezpečenie integrity používateľských dát pri prenose medzi dvoma dôveryhodnými systémami. Okrem kontroly integrity sa môže vyžadovať aj schopnosť opraviť niektoré typy chýb.

5.1.5 Identifikácia a autentifikácia (FIA)

Skupiny požiadaviek v tejto triede sa zameriavajú na funkcie na zistenie a overenie identity používateľa. Identifikácia (zistenie identity) a autentifikácia (overenie identity) sú základom pre priradenie správnych bezpečnostných atribútov používateľom. Sú nevyhnutným predpokladom na to, aby systém mohol presadzovať bezpečnostné politiky. Mnohé triedy požiadaviek sú závislé na správnej identifikácii a autentifikácii používateľov.

Neúspešná autentifikácia (FIA_AFL) Táto skupina požiadaviek sa zaoberá určením maximálneho počtu neúspešných pokusov o autentifikáciu a definovaním činností, ktoré sa udejú po prekročení tohto limitu, napr. znemožnenie ďalších pokusov o autentifikáciu z daného prístupového miesta na určený čas alebo až do vykonania nejakej činnosti administrátorom.

Definícia používateľských atribútov (FIA_ATD) Všetci oprávnení používatelia systému môžu mať definovanú množinu bezpečnostných atribútov (napr. členstvo v skupinách používateľov, roly, bezpečnostné oprávnenia na prístup k chráneným informáciám). Táto skupina obsahuje požiadavky na priraďovanie týchto bezpečnostných atribútov používateľom.

Špecifikácia tajných informácií (FIA_SOS) Na účely autentifikácie sa často používajú rôzne tajné informácie, ktorých znalosť umožnuje úspešne prejsť autentifikačným procesom. Táto skupina požiadaviek zabezpečuje bezpečnostné funkcie na kontrolu kvality tajných informácií a na generovanie tajných informácií, ktoré spĺňajú určené

kvalitatívne parametre. Napríklad pri heslách je potrebné, aby tieto neboli príliš jednoduché (napr. krátke postupnosti znakov z veľmi malej množiny) – môže sa vyžadovať napríklad minimálna dlžka, minimálny počet špeciálnych znakov a pod.

Autentifikácia používateľa (FIA_UAU) Táto skupina požiadaviek smeruje k zaisteniu autentifikácie používateľov. Môžu existovať činnosti, ktoré sú povolené aj bez autentifikácie používateľa, ale môžae sa aj vyžadovat, aby sa používateľ autentifikoval skôr, ako sa mu povolí akákoľvek ďalšia činost. Môže sa požadovatť, aby systém bol schopný detekovať alebo zabrániť použitiu autentifikačných údajov, ktoré boli falšované alebo skopírované (napríklad odpočutím hesla zo siete). Pre niektoré autentifikačné mechanizmy sa môže požadovať, aby nebolo možné viackrát použiť rovnaké autentifikačné dáta (napr. pri autentifikácii jednorazovými heslami). Môžu sa používať viaceré autentifikačné mechanizmy, potom je potrebné špecifikovať, akým spôsobom sa môžu použiť na autentifikáciu (napr. autentifikácia používateľa je úspešná, ak uvedie správne statické heslo a zároveň správne jednorazové heslo, alebo ak úspešne preukáže znalosť určeného súkromného kľúča, napr. použitím čipovej kryptografickej karty). Taktiež je možné požadovať, aby sa po určených udalostiach alebo pred vykonaním určených činností musel používateľ autentifikovať znova (napr. po 10 minútach neaktivity alebo pred zmenou autentifikačných údajov). Môže sa požadovať, aby používateľ od systému v priebehu autentifikačného procesu dostal len presne určené informácie (napr. len informáciu o úspechu alebo neúspechu identifikácie a autentifikácie a nie už informáciu o dôvode neúspechu - tým sa napríklad čiastočne staží možnosť skúšať kombinácie mien a hesiel, pretože útočník nevie, či vôbec skúšané meno v systéme existuje).

Identifikácia používateľa (FIA_UID) Táto skupina požiadaviek definuje podmienky, kedy sa musí používateľ identifikovat. Systém môže obsahovať nejaké činnosti, ktoré je možné vykonávať aj bez identifikácie používateľa (napr. prezeranie verejných dokumentov prostredníctvom Internetu), ale môže aj vyžadovať identifikáciu ako nutný predpoklad akejkoľvek inej činnosti používateľa.

Väzba medzi používateľom a subjektom (FIA_USB) Ľudský používateľ zvyčajne so systémom pracuje prostredníctvom procesu, ktorý vykonáva činnosti v mene používateľa a predstavuje subjekt systému, ktorý je viazaný na používateľa. Táto skupina požiadaviek špecifikuje, ako sa vytvára a udržiava prepojenie medzi bezpečnostnými atribútmi používateľa a subjektu, ktorý koná v mene používateľa.

5.1.6 Správa bezpečnosti (FMT)

Táto trieda má niekoľko cieľov:

- správa dát bezpečnostných funkcií
- správa bezpečnostných atribútov (napr. zoznamy prístupových práv)

- správa bezpečnostných funkcií (napr. výber funkcií a nastavovanie ich parametrov)
- definovanie bezpečnostných rôl

Správa funkcií (FMT_MOF) Táto skupina požiadaviek umožňuje oprávneným používateľom spravovať (povoľovat, zakazovať, nastavovať parametre) bezpečnostné funckie. Príkladom bezpečnostných funkcií sú napríklad funkcie bezpečnostného auditu, alebo funkcie na autentifikáciu. Spravovať bezpečnostné funkcie musí byť umožnené len používateľom, ktorí majú priradené určené bezpečnostné roly.

Správa bezpečnostných atribútov (FMT_MSA) Požiadavky tejto skupiny umožnujú oprávneným používateľom spravovať (prezerať, modifikovať) bezpečnostné atribúty. Spravovať bezpečnostné atribúty musí byť umožnené len používateľom, ktorí majú priradené určené bezpečnostné roly. Patria sem aj funkcie, ktoré kontrolujú správnosť bezpečnostných atribútov tak, aby nedošlo k porušeniu stanovených kritérií bezpečnosti. Taktiež sem patria funkcie, ktoré určujú prednastavené (default) bezpečnostné atribúty a umožnujú definovať bezpečnostné atribúty novo vytvoreným objektom a informáciam.

Správa dát bezpečnostných funkcií (FMT_MTD) Táto skupina požiadaviek umožňuje oprávneným používateľom spravovať (prezerať, meniť, mazať, ...) dáta bezpečnostných funkcií (konfiguračné parametre systému, hodiny, záznamy auditu, ...). Spravovať dáta bezpečnostných funkcií musí byť umožnené len používateľom, ktorí majú priradené určené bezpečnostné roly. Patria sem aj funkcie na nastavovanie limitov pre dáta bezpečnostných funkcií a definovanie činností, ktoré sa majú vykonať pri dosiahnutí, resp. prekročení nastavených limitov. Taktiež je možné požadovať, aby nastavované hodnoty boli kontrolované a neumožnilo sa nastavenie takých hodnôt, ktoré by viedli k porušeniu stanovených kritérií bezpečnosti.

Revokácia (rušenie) bezpečnostných atribútov (FMT_REV) Táto skupina poskytuje možnosť zrušiť bezpečnostné atribúty určených objektov, subjektov alebo iných prvkov systému. Rušenie bezpečnostných atribútov musí byť umožnené len používateľom, ktorí majú priradené určené bezpečnostné roly.

Expirácia bezpečnostných atribútov (FMT_SAE) Niektoré bezpečnostné atribúty môžu mať obmedzený čas platnosti. Táto skupina požiadaviek umožnuje oprávneným používateľom definovať obmedzenia na čas platnosti určených bezpečnostných atribútov a definuje, aká činnosť sa má vykonať, ked nejaký bezpečnostný atribút expiruje.

Bezpečnostné roly (FMT_SMR) Táto skupina požiadaviek riadi prideľovanie rôznych bezpečnostných rôl používateľom. Na bezpečnostné roly sa potom odvolávajú požiadavky na obmedzovanie oprávnení na vykonávanie činností. Môžu sa definovať aj požiadavky na vzájomné vzťahy medzi bezpečnostnými rolami (napr. aby rola administrátora bola nezlúčiteľná s rolou audítora oprávneného prezerať a mazať záznamy auditu).

Niektoré roly sa používateľom priradujú automaticky, iné môžu byť viazané na explicitnú požiadavku na priradenie bezpečnostnej roly.

5.1.7 Súkromie (FPR)

Táto trieda obsahuje skupiny požiadaviek, ktorých cieľom je poskytnúť používateľom ochranu proti zisteniu a zneužitiu ich identity inými používateľmi.

Anonymita (FPR_ANO) Táto skupina požiadaviek zabezpečuje, že používateľ môže používať určené služby systému bez toho, aby iné určené subjekty mali možnosť zistiť jeho identitu. Anonymita nechráni priamo identitu subjektu vykonávajúceho operácie, ale znemožnuje odhalenie väzby medzi identitou subjektu a skutočnou identitou používateľa.

Pseudoanonymita (FPR_PSE) Táto skupina požiadaviek zabezpečuje, že používateľ môže využívať určené služby systému bez toho, aby iné určené subjekty mali možnosť zistiť jeho identitu, ale umožnuje systému spojiť činnosti používateľa. Využívajú sa na to rôzne systémy aliasov – pseudonymov. Môže sa tiež vyžadovať, že oprávnený subjekt má mať možnosť zistiť skutočnú identitu používateľa.

Nespojiteľnosť (FPR_UNL) Táto skupina požiadaviek zabezpečuje, že určené subjekty nie sú schopné zistiť, či určené činnosti boli vykonané tým istým používateľom alebo majú inú určenú súvislosť.

Nepozorovateľnosť (FPR_UNO) Táto skupina požiadaviek zabezpečuje, že určené subjekty nie sú schopné zistiť, že chránený používateľ vykonáva určené činnosti s určenými objektami. Môže sa navyše požadovať, aby boli informácie o používateľovi rozložené v rôznych častiach systému, aby sa znížilo riziko zneužitia týchto informácií na porušenie nepozorovateľnosti v prípade získania neoprávneného prístupu k časti týchto informácií, prípadne sa môže požadovať, aby sa určité informácie o používateľovi vôbec nezisťovali. Tiež sa môže požadovať, aby oprávnený používateľ mal možnosť sledovať využívanie určených služieb.

5.1.8 Ochrana bezpečnostných funkcií (FPT)

Táto trieda požiadaviek obsahuje skupiny požiadaviek, ktorých cieľom je chrániť bezpečnostné funkcie a ich dáta. V istom zmysle sú tieto požiadavky podobné požiadavkám na ochranu používateľských dát a často sa aj realizujú podobnými alebo aj rovnakými prostriedkami. Avšak zatiaľ čo požiadavky na ochranu používateľských dát sledujú ochranu používateľských dát, požiadavky tejto triedy majú za úlohu zabezpečiť, že nie je možné obísť alebo neautorizovane upravovať bezpečnostnú politiku, ktorú bezpečnostné funkcie vynucujú a kontrolujú. Bez adekvátnej ochrany bezpečnostných funkcií a ich dát

nie je možné bezpečné fungovanie systému zaistiť. Napríklad, ak je možné neautorizovane meniť heslá, nemá zmysel používať autentifikáciu založenú na znalosti hesiel. Ak je možné neautorizovane zmeniť implementáciu bezpečnostných funkcií, je možné ich zmeniť tak, že povolia činnosti v rozpore s príslušnou politikou. Ochrana bezpečnostných funkcií sa týka troch významných oblastí:

- abstraktný počítač - virtuálny alebo fyzický počítač, na ktorom pracuje implementácia bezpečnostných funkcií (napr. samotný hardware, hardware + operačný systém, implementácia virtuálneho počítača a pod.),
- implemetnácia bezpečnostných funkcií, ktorá pracuje na abstraktnom počítači a implementuje mechanizmy, ktorými sa vynucuje a kontroluje bezpečnostná politika,
- dáta bezpečnostných funkcií, ktoré riadia správanie bezpečnostných funkcií.

Test abstraktého počítača (FPT_AMT) Táto skupina definuje požiadavky na vykonávanie testov abstraktného počítača, ktorých cieľom je overiť bezpečnostné predpoklady, ktorých splnenie je nutné na bezpečné fungovanie bezpečnostných funkcií. Abstraktným počítačom môže byť napríklad hardvér, hardvér+firmvér, ale aj zložitejšia kombinácia hardvéru a softvéru, ktorá z pohľadu bezpečnostných funkcií funguje ako virtuálny počítač. Špecifikuje sa aké testy sa majú vykonať a kedy (napr. pri spustení systému, pravidelne, na vyžiadanie oprávneného používateľa).

Zachovanie bezpečnosti pri poruchách (FPT_FLS) Táto skupina požiadaviek zabezpečuje, aby systém zostal v stave, kedy nedôjde k porušeniu bezpečnostnej politiky ani v prípade, ked dôjde k určeným typom porúch alebo chýb (napr. sa vyčerpajú nejaké zdroje alebo sa pokazí nejaké hardvérové zariadenie).

Dostupnosť exportovaných dát bezpečnostných funkcií (FPT_ITA) Táto skupina požiadaviek zabezpečuje, aby určené dáta bezpečnostných funkcií, ktoré využívajú iné dôveryhodné IKT produkty, boli týmto produktom za určených podmienok v potrebnej miere dostupné. Napríklad systém môže spravovať databázu autentifikačných informácií (heslá, verejné kľúče, ...) a tieto poskytovať iným systémom, ktoré ich potrebujú. Potom sa v rámci tejto skupiny môže napr. požadovať, aby tieto autentifikačné informácie boli dostupné, ak fungujú aspoň v určitej miere komunikačné linky a funguje aspoň jeden z dvojice diskov, kde sú tieto informácie uložené.

Dôvernosť exportovaných dát bezpečnostných funkcií (FPT_ITC) Táto skupina požiadaviek sa zaoberá zachovaním dôvernosti dát bezpečnostných funkcií prenášaných do iného systému.

Integrita exportovaných dát bezpečnostných funckií (FPT_ITI) Táto skupina požiadaviek sa zaoberá kontrolou integrity dát bezpečnostných funkcií pri ich prenose do iného systému a činnosťami, ktoré sa majú vykonať v prípade porušenia integrity. Môže sa tiež požadovať schopnosť opravy niektorých typov chýb.

Vnútorné prenosy dát bezpečnostných funkcií (FPT_ITT) Táto skupina požiadaviek sa zaoberá ochranou dát bezpečnostných funkcií pri ich prenose medzi rôznymi časťami systému. Ochrana sa týka dôvernosti a integrity týchto dát. Môže sa tiež požadovať, aby na ich prenos bol využívaný iný komunikačný kanál, než ktorý sa využíva na prenos používateľských dát.

Fyzická ochrana bezpečnostných funkcií (FPT_PHP) Fyzická ochrana sa zameriava na obmedzenie alebo znemožnenie fyzického prístupu k zariadeniu vykonávajúcemu bezpečnostné funkcie. Taktiež sem patria požiadavky na odolnosť voči fyzickým zásahom alebo pokusom o zámenu časti zariadenia vykonávajúceho bezpečnostné funkcie. Môže sa požadovať pasívna detekcia fyzickej manipulácie, ktorá umožnuje zistiť, že k nejakej manipulácii došlo (napr. plomby), aktívne monitorovanie pokusov o fyzickú manipuláciu a ich ohlasovanie určeným spôsobom (napr. elektronický zabezpečovací systém), ale aj odolnosť voči určitým typom fyzických útokov, pri ktorých sa požaduje zachovanie bezpečného stavu (napr. použitie obalu, ktorý odolá určitým nástrojom na jeho porušenie a v prípade použitia prostriedkov, ktorým neodolá, vymazanie dát, ktorých dôvernosť je kritická).

Bezpečné zotavenie (FPT_RCV) Požiadavky tejto skupiny sa týkajú potreby bezpečného štartu systému a jeho zotavenia po prerušení činnosti. Tieto sú dôležité, pretože stav systému pri štarte výrazne ovplyvňuje ochranu jeho stavu počas prevádzky. Na bezpečné zotavenie sa môže vyžadovať ľudský zásah alebo sa môže vyžadovať schopnosť bezpečného zotavenia z určených druhov prerušení prevádzky – ľudský zásah sa potom vyžaduje len v prípade, keď automatické zotavenie nebolo možné. Taktiež sa môže požadovat, aby systém bol schopný obmedziť možné straty následkom prerušenia činnosti na určitú hranicu. Patria sem aj požiadavky, aby bezpečnostné funkcie buď úspešne skončili alebo, pri identifikovaných chybách a poruchách, uviedli systém do predchádzajúceho konzistentného stavu.

Detekcia opakovania (replay) (FPT_RPL) Do tejto skupiny patria požiadavky na schopnosť detekovať opakované správy, požiadavky na služby, odpovede na požiadavky a pod. Taktiež sa tu definujú činnosti, ktoré sa majú vykonať v prípade opakovania. Schopnosť detekovať tieto opakovania znemožnuje ich zneužie – replay útoky. Príkladom môže byť pokus o použitie už použitého jednorazového hesla alebo šifrovacieho kľúča.

Reference mediation (FPT_RVM) Táto skupina obahuje požiadavky na zabezpečenie toho, že žiadnu činnosť, ktorej sa týka určitá bezpečnostná politika, nemôže žiad-

ny subjekt (okrem špeciálnych privilegovaných subjektov) vykonať bez toho, aby o tom rozhodla bezpečnostná funkcia implementujúca príslušnú bezpečnostnú politiku.

Separácia domén (FPT_SEP) Táto skupina obsahuje požiadavky na existenciu rôznych bezpečnostných domén, ktoré znemožňujú interakcie (sledovanie činnosti, dát, modifikácia dát alebo vykonateľného kódu a pod.) subjektov a objektov patriacich do rôznych bezpečnostných domén. Prechody medzi bezpečnostnými doménami musia byť možné len prostredníctvom príslušných bezpečnostných funkcií.

Protokol na synchronizáciu stavu (FPT_SSP) V distribuovaných systémoch je potrebné zabezpečiť synchronizáciu stavu medzi jednotlivými časťami systému. Táto skupina obsahuje požiadavky orientované na existenciu a využívanie bezpečného protokolu, ktorý zabezpečuje, že všetky relevantné časti distribuovaného systému majú synchronizovaný stav po všetkých bezpečnostne relevantných udalostiach. Napr. ked si používateľ zmení heslo na jednom počítači, ktorý je súčasťou siete počítačov, ktoré majú používať spoločné informácie o heslách, je potrebné, aby sa o tejto zmene dozvedeli aj ostatné počítače a aby sa ten prvý dozvedel o tom, že ostatné už túto informáciu dostali. Inak by mohla nastať situácia, že používateľ si myslí, že si úspešne zmenil heslo, no niektoré počítače sa o tejto zmene nedozvedeli a je možné ich prostredníctvom pristupovať do systému so starým heslom.

Časové pečiatky (FPT_STM) Táto skupina obsahuje požiadavky na existenciu bezpečnostných funkcií umožňujúcich získať spoľahlivú informáciu o aktuálnom čase pre potreby iných bezpečnostných funkcií (napr. pre generovanie záznamov auditu).

Konzistencia dát bezpečnostných funkcií pri prenose (FPT_TDC) Táto skupina obsahuje požiadavky na správnu a konzistentnú interpretáciu dát bezpečnostných funkcií, ktoré sú zdieľané alebo prenášané medzi viacerými dôveryhodnými systémami.

Konzistencia dát bezpečnostných funkcií pri replikácii (FPT_TRC) Táto skupina obsahuje požiadavky na zachovanie konzistencie dát bezpečnostných funkcií, keď sa tieto replikujú do viacerých častí systému. V prípade, že napr. následkom zlyhania vnútorného komunikačného kanála, dôjde k situácii, že tieto dáta nie sú konzistentné, bezpečnostné funkcie musia zabezpečiť zosúladenie kópií týchto dát na rôznych miestach po opätovnom obnovení komunikácie medzi časťami systému.

Testovanie bezpečnostných funkcií (FPT_TST) Táto skupina obsahuje požiadavky na testovanie bezpečnostných funkcií s cieľom zistit, či pracujú správne. Testy zahŕňajú napr. aj testy integrity dát bezpečnostných funkcií a integrity a autenticity vykonateľného kódu. Testy sa môžu vykonávať pri spustení, pravidelne, na vyžiadanie oprávneného používateľa alebo v iných špecifikovaných situáciach.

5.1.9 Využívanie zdrojov (FRU)

Odolnosť voči poruchám (FRU_FLT) Požiadavky tejto skupiny majú za cieľ zabezpečiť fungovanie systému aj v prípade porúch. V prípade špecifikovaných porúch sa môže vyžadovať zachovanie plnej funkčnosti systému alebo niektorých jeho častí.

Priorita služieb (FRU_PRS) V rámci tejto skupiny požiadaviek sa požaduje priradenie priorít všetkým subjektom a následne riadenie využívania zdrojov (výpočtová kapacita, pamäťový priestor, ...) na základe týchto priorít. Tým sa zabezpečuje, že činnosti vykonávané subjektami s vyššou prioritou sa budú môcť vykonať bez zbytočného odkladu spôsobeného vykonávaním činností subjektami s nižšou prioritou.

Alokácia zdrojov (FRU_RSA) Táto skupina požiadaviek poskytuje limity na využívanie obmedzených zdrojov pre jednotlivé subjekty alebo typy subjektov. Určený subjekt nemôže použiť viac ako mu jeho limit pre daný typ zdrojov umožnuje, čím sa zabraňuje tomu, aby mohol vyčerpať celú kapacitu zdrojov a znemožniť tým činnosti iných subjektov. Môže sa tiež požadovat, aby určené subjekty vždy mali k dispozícii aspon nejakú určenú minimálnu kapacitu daného zdroja.

5.1.10 Prístup k systému (FTA)

Obmedzenie rozsahu voliteľných atribútov (FTA_LSA) Táto skupina obsahuje požiadavky na obmedzenie toho, aké bezpečnostné aribúty relácie (alebo ich kombinácie) si môže používateľ zvoliť pri vytváraní relácie.

Obmedzenie viacnásobných relácií (session) (FTA_MCS) Táto skupina obsahuje požiadavky na obmedzenia počtu relácií, ktoré môže mať jeden používateľ súčasne.

Uzamykanie relácie (session) (FTA_SSL) Táto skupina obsahuje požiadavky na uzamykanie relácie po určenom čase nečinnosti používateľa alebo na jeho žiadost. Tiež je možné požadovať schopnosť systému ukončiť reláciu používateľa po určenom čase nečinnosti.

Prístupové oznamy (FTA_TAB) Táto skupina obsahuje požiadavky na zobrazovanie oznamov a/alebo varovaní týkajúcich sa použitia systému pred vytvorením používateľskej relácie (pred prihlásením).

História prístupu (FTA_TAH) Táto skupina obsahuje požiadavky na zobrazenie posledného úspešného a neúspešného vytvorenie relácie po úspešnom vytvorení relácie. Zobrazovať sa môžu informácie ako dátum a čas, typ relácie, mieto, odkial bola relácie vytvorená.

Vytváranie relácie (session) (FTA_TSE) Táto skupina definuje požiadavky na možnosť zakázať vytvorenie relácie používateľovi na základe určených podmienok (napr. čas, miesto, odkial sa snaží reláciu vytvoriť a pod.).

Dôveryhodná cesta a kanál (FTP) Táto trieda požiadaviek obsahuje skupiny zamerané na existenciu a využívanie dôveryhodných komunikačných kanálov medzi bezpečnostnými funkciami a inými dôveryhodnými systémami a dôveryhodných komunikačných ciest medzi bezpečnostnými funkciami a používateľmi.

Dôveryhodný kanál (FTP_ITC) Dôveryhodný komunikačný kanál je komunikačný kanál, ktorý poskytuje spoľahlivú identifikáciu oboch strán a zabezpečuje ochranu prenášaných údajov pred porušením dôvernosti alebo integrity. Táto skupina obsahuje požiadavky na existenciu a využívanie dôveryhodných komunikačných kanálov medzi bezpečnostnými funkciami a inými dôveryhodnými IKT produktami.

Dôveryhodná cesta (FTP_TRP) Táto skupina definuje požiadavky na vytváranie a udržiavanie dôveryhodnej komunikačnej cesty medzi bezpečnostnou funkciou a používateľom. Dôveryhodná komunikačná cesta je komunikačná cesta medzi bezpečnostnou funkciou a používateľom, ktorá zabezpečuje spoľahlivú identifikáciu oboch strán a ochranu prenášaných údajov proti porušeniu dôvernosti a integrity. Dôveryhodná cesta je napríklad potrebná pre prenos citlivých informácií (ako napr. heslo) od používateľa k bezpečnostnej funkcii. Znemožnuje napríklad, aby niekto nechal na počítači bežať program, ktorý iný používateľ nerozozná od štandardného pogramu slúžiaceho na prihlásenie do systému a odovzdá mu svoje heslo.

5.1.11 Príklad použitia funkcionálnych požiadaviek

Na malom príklade ukážeme, že jednotlivé požiadavky medzi sebou súvisia a nie je ich možné použiť izolovane. Predpokladajme, že jedným z bezpečnostných cieľov systému je možnosť určenia zodpovednosti za činnosti, teda možnosť spoľahlivo určiť, ktorý používateľ vykonal určité činnosti. Na to potrebujeme pre systém vybrať požiadavky z triedy FAU (Bezpečnostný audit). Potrebujeme, aby systém vytváral záznamy auditu (FAU_GEN) pre každú činnost, ktorej vykonávanie chceme sledovat. Záznamy auditu musia obsahovať aj identifikáciu používateľa, ktorý činnosť vykonal a čas, kedy k jej vykonaniu došlo. Z toho vyplýva, požiadavka na časové pečiatky (FPT_STM) a požiadavka na identifikáciu používateľa pred vykonávaním sledovaných činností (FIA_UID). Aby bolo zaistené, že používateľ nemôže predstierať falošnú identitu, je potrebné požadovať autentifikáciu (FAU_UAU), a potrebujeme zabezpečiť väzbu medzi identitou používateľa a jeho procesmi (FIA_USB). Taktiež budeme zrejme potrebovať definovať určité bezpečnostné atribúty používateľom (FIA_ATD). Na autentifikáciu budeme potrebovať nejaké tajné údaje (napr. predpokladajme autentifikáciu heslom), ktoré musia splnať určité kritéria (FIA_SOS). Budeme potrebovať spravovať bezpečnostné atribúty a dáta bezpečnostných funkcií (napr. heslá, prístupové práva) – FMT_MTD, FMT_MSA, ovládať a konfigurovať funkcie auditu - FMT_MOF. K záznamom auditu a autentifikačným

informáciam nemôže mať prístup ktokoľvek, teda potrebudejeme rôzne bezpečnostné roly - FMT_SMR. Záznamy auditu sa musia niekde ukladať (FAU_STG) a musia sa dať prezerať (FAU_SAR). Ak chceme, aby nebolo možné bezpečnostné funkcie, ktoré budú realizovať uvedené požiadavky obísť alebo zmenit, aby bolo možné udržať záznamy auditu ochránené pred neoprávnenou modifikáciou, aby nebolo možné neoprávnene zasahovať do autentifikačných údajov a pod., potrebujeme aj mnohé požiadavky z triedy FPT (Ochrana bezpečnostných funkcií), a aby používatelia mohli bezpečne absolvovať autentifikáciu, bude potrebné realizovať aj dôveryhodnú komunikačnú cestu (FTP_TRP). Ako vidieť, z jedného bezpečnostného cieľa, ktorý sa vôbec netýkal priamej ochrany používateľských dát, vyplynula potreba pomerne širokého spektra funkcionálnych bezpečnostných požiadaviek.

5.2 Požiadavky na bezpečnostné záruky

V predchádzajúcich častiach tohto dokumentu sme popísali bezpečnostné potreby systému: či už vyplývajúce z hrozieb voči jednotlivým položkám systému, alebo z dokumentov, ktoré sú pre prevádzku systému záväzné. Tieto sa premietli do bezpečnostných cieľov systému (a jeho bezpečnostného prostredia) a na ich realizáciu boli prijaté isté opatrenia, ktoré mali podobu bezpečnostných požiadaviek. Bezpečnosť IKT systému však nemožno zaistiť, ak zostanú nepokryté nejaké hrozby voči systému, resp. ak budú navrhované opatrenia síce adekvátne bezpečnostným cieľom systému, ale ich realizácia nedosiahne potrebnú kvalitatívnu úroveň. Preto je súčasťou bezpečnostného modelu systému aj stanovenie požiadaviek na bezpečnostné záruky. Bezpečnostné záruky vyjadrujú stupeň dôvery v to, že systém spĺňa bezpečnostné požiadavky. Bezpečnostné záruky sa určujú na základe aktívneho odborného posudzovania (evaluácie) systému. Na zaistenie toho, aby boli bezpečnostné záruky úplné, konzistentné a kvantitatívne vyjadritelné, používajú Common Criteria podobnú filozofiu ako pre funkcionálne bezpečnostné požiadavky. Definujú triedy požiadaviek na bezpečnostné záruky [4] a stanovujú 7 hierarchicky usporiadaných úrovní bezpečnostných záruk (Evaluation assurance level, EAL). Na to, aby hodnotený IKT systém dosiahol niektorú z úrovní EAL, musí spĺňať požiadavky na bezpečnostné záruky prislúchajúce príslušnej triede. Požiadavky na bezpečnostné záruky môžu byť užitočné nielen pre IKT systémy, ktoré sa uchádzajú o akreditáciu, ale aj na zaistenie potrebnej úrovne bezpečnosti bežne prevádzkovaných IKT systémov, u ktorých nie je ani reálne ani potrebné dosiahnuť formálnu akreditáciu. Stručne popíšeme triedy požiadaviek na bezpečnostné záruky. Samotné úrovne záruk nebudeme rozoberat, čitateľa odkazujeme na [5].

5.2.1 Manažment konfigurácie (ACM)

Manažment konfigurácie (IK systému) pomáha zaistiť zachovanie integrity systému. Vyžaduje disciplínu a riadenie procesov úprav a modifikácie systému a informácií súvisiacich so systémom (napr. dokumentácie.) Manažment konfigurácie zabranuje neoprávneným modifikáciám (pridávaniu alebo odoberaniu častí, komponentov, údajov a pod.) systému a poskytuje záruku, že IK systém je v stave deklarovanom jeho dokumentáciou.

5.2.2 Dodávka a prevádzka (ADO)

Trieda záruk ADO definuje požiadavky na opatrenia, procedúry a štandardy týkajúce sa bezpečného doručenia, inštalácie a prevádzky systému. Garantuje, že nedošlo ku kompromitácii bezpečnostných funkcií systému počas prevozu, inštalácie, spustenia do prevádzky a samotnej prevádzky. Požiadavky triedy ADO sú aktuálne pri obstarávaní systému (hardvér, softvér, firmvér) od externého dodávateľa, pri dodávke softvéru vytvoreného pomocou vlastných programátorských kapacít, ako aj pri prevádzke samtného IKT systému.

5.2.3 Vývoj (ADV)

Trieda záruk ADV definuje požiadavky na postupné zjemnovanie popisu systému, počínajúc jeho funkcionálnou špecifikáciou a končiac skutočnou implementáciou systému. Každá z reprezentácií systému by mala obsahovať dostatok informácií na to, aby sa dalo posúdiť, či boli splnené funkcionálne požiadavky na system.

5.2.4 Dokumentácia (AGV)

Trieda AGV defiuje požiadavky na rozsah, zrozumitelnosť a úplnosť dokumentácie, ktorú poskytuje tvorca systému. Dokumentácia sa delí na dokumentáciu pre administrátorov systému a dokumentáciu pre používateľov a je dôležitým predpokladom bezpečnej prevádzky systému.

5.2.5 Podpora v priebehu životného cyklu (ALC)

Trieda ALC definuje požiadaky na záruky prostredníctvom použitia dobre definovaného modelu celoživotného cyklu systému pokrývajúceho všetky etapy vývoja systému. Zahŕňa politiky a procedúry odstraňovania zistených nedostatkov, korektné používanie nástrojov a techník a bezpečnostné opatrenia na ochranu vývojového prostredia.

5.2.6 Testy (ATE)

Trieda ATE stanovuje požiadavky na testovanie, ktoré má demonštrovať, že bezpečnostné funkcie systému spĺňajú bezpečnostné funkcionálne požiadavky systému.

5.2.7 Ohodnotenie slabých miest (AVA)

Trieda AVA definuje požadavky zamerané na identifikáciu využiteľných slabých miest systému. Zaoberá sa slabými miestami, ktoré vznikajú pri konštrukcii, prevádzke, zneužití alebo nesprávnej konfigurácii systému.

5.2.8 Udržiavanie záruk (AMA)

Trieda AMA je zameraná na udržiavanie úrovne záruk. Systém by mal spĺňať svoje bezpečnostné ciele aj po tom, ako sa uskutočnia zmeny v systéme alebo v jeho bezpečnostnom prostredí.

Okrem uvedených tried záruk existujú dalšie dve triedy záruk, ktorých použitelnosť pre hodnotenie bezpečnosti konkrétneho IK systému je obmedzená.

5.2.9 Hodnotenie Protection Profile (APE)

Protection profile je bezpečnostný model abstraktného systému (čipovej karty, operačného systému, firewall-u). Špecifikuje (bezpečnostné) požiadavky, ktoré by malo konkrétne riešenie daného systému spĺňať. Hodnotenie PP má demonštrovat, že PP je úplný, konzistentný, technicky vyhovujúci a preto vhodný na formulovanie požiadaviek na system. PP, ktorý prešiel úspešne hodnotením sa môže stať základom pre vypracovanie bezpečnostného zámeru systému.

5.2.10 Hodnotenie bezpečnostného zámeru (ASE)

Bezpečnostný zámer (Security target) je množina bezpečnostných požiadaviek a špecifikácií, nejakého systému, ktoré sa majú použiť ako základ jeho hodnotenia.

Common Criteria definujú 7 úrovní bezpečnostných záruk (Evaluation Assurance Level, EAL). Na to, aby bolo možné system certifikovať na niektorej z úrovní EAL, je potrebné, aby spĺňal požiadavky na bezpečnostné záruky pre príslušnú triedu. Úrovne záruk EAL sú hierarchicky usporiadané (vzostupne); na zaradenie do vyššej úrovne je potrebné splniť väčší rozsah požiadaviek na záruky, evaluácia systému musí ísť do väčšej hlbky a používať exaktnejšie (formálne) metódy. Úrovnami záruk sa nebudeme zaoberať, čitateľ nájde potrebné informácie v [5].

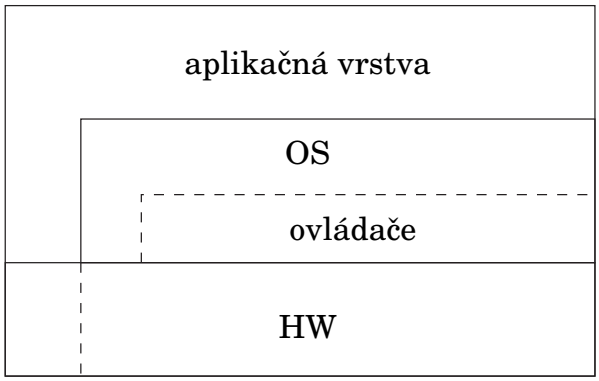
Časť II

Bezpečnostné aspekty operačných systémov

Kapitola 6

Úloha operačného systému v bezpečnosti

Informačné systémy, či už sa jedná o veľké integrované systémy alebo o sadu samostatných programov, z pohľadu ich fungovania pozostávajú z niekoľkých vrstiev (obr. 6.1). Charakteristickou vlastnosťou týchto vrstiev je, že nižšie vrstvy poskytujú prostredníctvom určitého definovaného rozhrania určité služby vyšším vrstvám. Z hľadiska informačnej bezpečnosti, ako uvidíme, je dôležitou vlastnosťou vrstvy izolácia vrstiev nad ňou od priameho nekontrolovaného využívania služieb poskytovaných vrstvami pod ňou. Samozrejme, vrstva môže sprístupniť vymedzenú časť funkcií nižšej vrstvy aj pre priame použitie vyššou vrstvou – napr. aplikácie bežne môžu používať priamo časť procesora. Spodnú vrstvu tvorí hardvér, na ktorom je systém prevádzkovaný. V hardvérovej vrstve sa skutočne nachádzajú všetky uložené a spracovávané informácie. Nad ňou je vrstva tvorená operačným systémom. Túto môže byť niekedy vhodné vnímať ako dve vrstvy, nižšiu – hardvérovo závislú – tvorenú ovládačmi zariadení, a vyššiu – hardvérovo nezávislú, ktorá definuje služby poskytované operačným systémom. Nad operačným systémom sa nachádza aplikačná vrstva tvorená aplikačnými programami, ktoré realizujú funkciu informačného systému.



Obrázok 6.1: Vrstvy informačného systému

Aplikačná vrstva môže byť z hľadiska poskytovania a využívania služieb, ako aj z hľadiska izolácie niekedy vnímaná ako viac vrstiev. Príkladom môže byť aplikácia využívajúca služby databázového servera. Databázový server poskytuje aplikácii služby na manipuláciu s údajmi a zároveň plní izolačnú funkciu – umožňuje aplikácii manipulovať s údajmi len definovaným spôsobom. Takéto členenie je však špecifické pre daný typ aplikácie, nie je univerzálne, ako oddelenie vrstvy operačného systému. Niekedy môže byť vhodnejšie sa na spoluprácu aplikácie s databázovým serverom pozerať ako na komunikáciu dvoch samostatných procesov na aplikačnej vrstve použitím prostriedkov operačného systému. Z hľadiska toku údajov a využívania funkcií operačného systému je takýto pohľad presnejší; z hľadiska rozhodovania o mieste implementácie bezpečnostných funkcií môže byť vhodnejší model databázovej vrstvy.

Programy na aplikačnej vrstve (podobne aj operačný systém), môžu byť z hľadiska svojej vnútornej štruktúry tiež členené na vrstvy. Typickým príkladom takéhoto členenia sú knižnice funkcií[1], ktoré aplikácia využíva. Tieto však bežne nemajú izolačnú funkciu, ktorá by skutočne bránila aplikácii v prístupe k službám nižšej vrstvy – napr. aplikácia namiesto použitia knižničnej funkcie môže priamo použiť volania operačného systému. Z hľadiska úlohy operačného systému v bezpečnosti nie sú takéto delenia aplikačnej vrstvy podstatné, preto sa nimi nebudeme zaoberať.

Vlastnosti nižších vrstiev majú rozhodujúci vplyv na možnosť účinnej realizácie bezpečnostných funkcií na vyšších vrstvách. Predpokladom účinnej realizácie bezpečnostnej funkcie je splnenie niekoľkých základných podmienok:

- bezpečnostnú funkciu nie je možné "obísť", t.j. subjekt, ktorého činnosť podlieha schváleniu bezpečnostnou funkciou, nesmie mať možnosť túto činnosť vykonať bez schválenia bezpečnostnou funkciou,
- bezpečnostná funkcia musí byť chránená proti neoprávnenej manipulácii s jej implementáciou, t.j. neoprávnený subjekt nesmie mať možnosť zmeniť implementáciu bezpečnostnej funkcie – inak by ju mohol zmeniť tak, že umožní vykonať činnosti, ktoré by inak nedovolila, alebo neumožní oprávneným subjektom vykonať činnosti, ktorý by im inak vykonať umožnila,
- informácie, na základe ktorých bezpečnostná funkcia realizuje rozhodnutia, musia byť chránené pred neoprávnenou manipuláciou, napr. neoprávnený subjekt nesmie mať možnosť zmeniť tieto údaje tak, aby následne bezpečnostná funkcia umožnila vykonať činnosť, ktorú by inak vykonať nepovolila, alebo naopak neumožnila oprávnenému subjektu vykonať činnosť, ktorú by inak vykonať mohol,
- dôverné informácie, ktoré bezpečnostná funkcia využíva napr. na účely autentifikácie subjektu, musia byť chránené pred neoprávneným prístupom.

Ak má byť určitá bezpečnostná funkcia realizovaná na určitej vrstve, je potrebné, aby buď potenciálny útočník nemal priamy prístup k službám nižších vrstiev, alebo aby nižšie vrstvy zabezpečovali splnenie uvedených podmienok. Túto skutočnosť ukážeme na niekoľkých príkladoch.

[1] alebo, pri objektovo orientovaných knižniciach, tried

Napríklad predpokladajme, že nad operačným systémom, ktorý neobsahuje bezpečnostné funkcie riadenia prístupu lokálnych používateľov[2], by sme chceli prevádzkovať aplikáciu, ktorá by poskytovala prístup k určitým informáciam uloženým na lokálnom disku počítača, pričom by realizovala identifikáciu a autentifikáciu používateľov a riadenie ich prístupu k týmto informáciam. Ak táto aplikácia bude poskytovať svoje služby prostredníctvom počítačovej siete a prístup k službám operačného systému (či už fyzickým prístupom k počítaču alebo prostredníctvom sieťových služieb) budú mať len subjekty oprávnené na prístup k všetkým informáciam uloženým na lokálnom disku, bude aplikácia predstavovať izoláciu útočníka od služieb nižších vrstiev a jej bezpečnostné funkcie môžu byť účinné. Ak však potenciálny útočník má prístup k službám operačného systému, nemusí na prístup k informáciam použiť služby aplikácie, ale služby operačného systému, čím sa vyhne riadeniu prístupu realizovanému v aplikácii.

Pozrime sa teraz na príklad, ktorý na prvý pohľad vyzerá výrazne bezpečnejšie, no v skutočnosti má od bezpečného ďaleko. Predpokladajme opäť rovnaký operačný systém a pozrime sa na možnosť realizácie aplikácie na vytváranie elektronického (digitálneho) podpisu. Na ochranu súkromného kľúča sa využije externé hardvérové zariadenie – čipová karta, ktorá neumožňuje export súkromného kľúča, ale poskytuje službu vytvorenie elektronického podpisu po prenesení hašovacej hodnoty dokumentu. Pred tým, ako čipová karta umožní využitie tejto služby, požaduje zadanie hesla alebo PIN-u, čo slúži na autentifikáciu oprávneného používateľa. Aplikácia v počítači plní úlohu rozhrania medzi používateľom a čipovou kartou – jej úlohou je získať od používateľa dokument, vypočítať z neho hašovaciu hodnotu, získať od používateľa heslo alebo PIN, odoslať tieto informácie do karty a následne z nej prijať hodnotu elektronického podpisu a vytvoriť výsledný podpísaný dokument v požadovanom formáte. Útočník, ktorý má prístup k službám operačného systému, môže napr. modifikovať uvedenú aplikáciu tak, aby po získaní hesla alebo PINu od používateľa túto informáciu poskytla útočníkovi, alebo aby nechala podpísať útočníkom pripravený dokument.

Uvedené príklady demonštrujú, že pokiaľ operačný systém neposkytuje prostriedky ochrany súborov pred neoprávneným prístupom, na aplikačnej vrstve je takúto ochranu účinnú aj proti lokálnym používateľom prakticky nemožné implementovať. Podobne, ak operačný systém neposkytuje prostriedky na ochranu integrity aplikácií, je prakticky nemožné implementovať aplikáciu, ktorá by ochránila dôvernosť informácií, ktoré spracováva, pred inými používateľmi systému. Príklady vychádzali z predpokladu, že operačný systém neposkytoval bezpečnostné funkcie riadenia prístupu lokálnych používateľov. Avšak ani v prípade operačného systému, ktorý tieto prostriedky poskytuje[3], nemusí byť táto ochrana, ako uvidíme v ďalších kapitolách, dostatočná. Jednoznačne vidíme, že bezpečnostné funkcie operačného systému výrazne ovplyvňujú, čo je možné dosiahnuť na aplikačnej úrovni.

Ak má operačný systém účinne realizovať bezpečnostné funkcie, musí zabezpečiť aj ochranu vlastných bezpečnostných funkcií a informácií ovplyvňujúcich ich rozhodovanie. Musí ich chrániť pred narušením prostriedkami operačného systému aj prostriedkami hardvérovej vrstvy. Väčšina operačných systémov neizoluje aplikačnú vrstvu od hard-

[2]Príkladom takéhoto operačného systému je Microsoft Windows 98, ktorý stále patrí medzi pomerne rozšírené operačné systémy, najmä medzi domácimi používateľmi a v malých firmách.

[3]Napr. Linux, všetky systémy typu UNIX, Microsoft Windows 2000.

véru úplne, t.j. aplikačné programy priamo využívajú časť hardvéru (najmä procesor)[4]. Preto je veľmi dôležité, aby aplikácie nemohli zneužiť prístup k hardvéru na "obídenie" operačného systému. Ak napríklad aplikačný program môže pristupovať do pamäte využívanej operačným systémom, môže zmeniť jeho implementáciu alebo manipulovať s jeho informáciami. Na zabránenie takýchto nežiadúcich zásahov z aplikačnej vrstvy do operačného systému je potrebné, aby hardvérová vrstva umožňovala operačnému systému obmedziť funkcie hardvérovej vrstvy poskytnuté aplikačnej vrstve. Dnešné bežné procesory takéto funkcie majú – umožňujú vymedziť časť pamäte, ktorá je procesu prístupná, a obmedzujú používanie privilegovaných inštrukcií[5] len na oprávnené procesy (zvyčajne operačný systém).

Nezanedbateľným aspektom ochrany informácií a implementácie bezpečnostných funkcií je aj ochrana v čase, keď hardvérová vrstva nie je pod kontrolou operačného systému, resp. ochrana proti prístupu k hardvérovej vrstve prostriedkami, ktoré nie sú pod kontrolou operačného systému (napr. priama manipulácia s hardvérom, prenesenie pevného disku do iného počítača, a pod.). Najčastejším riešením sú prostriedky fyzickej bezpečnosti, ktorými sa bráni fyzickému prístupu útočníka k hardvéru. Keď to nie je vhodné alebo možné, alebo keď je potrebná ochrana aj proti útočníkovi, ktorý má fyzický prístup k hardvéru, je možné využiť kryptografické prostriedky spomenuté v časti 2.1 pri jednotlivých aspektoch ochrany. Operačný systém však môže spoľahlivo overiť autentickosť informácií alebo svojich súčastí len ak je zabezpečené, že tie časti operačného systému a informácie, ktoré sa pri overovaní využívajú, neboli modifikované. To sa dá zabezpečiť jedine na hardvérovej vrstve alebo tak, že sa základ operačného systému načítava z nemodifikovateľného pamäťového média.

[4]Existuje aj možnosť úplnej izolácie aplikačnej vrstvy od hardvérovej, keď operačný systém implementuje virtuálny počítač, ktorý vykonáva inštrukcie aplikačných programov. Toto riešenie je v porovnaní s priamym využívaním procesora aplikačnou vrstvou pomalšie, na druhej strane umožňuje úplnú nezávislosť aplikácií na hardvérovej platforme. Operačné systémy, ktorým sa budeme v tejto práci bližšie venovať, týmto spôsobom nepracujú.

[5]napr. inštrukcie ovplyvňujúce vymedzenie pamäte procesu, inštrukcie na prístup k iným častiam hardvéru, a pod.

Kapitola 7

Bezpečnostné funkcie bežných operačných systémov

V predchádzajúcej kapitole sme poukázali na dôležitú úlohu operačného systému pre bezpečnosť informačného systému ako celku. V tejto kapitole sa pozrieme na bezpečnostné funkcie implementované niektorými bežnými operačnými systémami. Vyberieme tri skupiny operačných systémov obsahujúce najpoužívanejšie operačné systémy na počítačoch architektúry Intel – dve skupiny obsahujú proprietárne operačné systémy Microsoft Windows – jednu skupinu tvoria operačné systémy Microsoft Windows 95/98, druhú Microsoft Windows NT/2000/XP. Tretiu tvorí operačný systém Linux[1] zo skupiny Open Source produktov. Mnoho z vlastností Linux-u však majú aj všetky operačné systémy typu UNIX.

Ako základnú schému pre popísanie bezpečnostných funkcií jednotlivých skupín operačných systémov použijeme štandard Common Criteria, ktorému sme sa venovali v kapitole 5. Pozrieme sa postupne na každú triedu funkčných požiadaviek a popíšeme, ktoré z funkčných požiadaviek patriacich do tejto triedy sú v popisovaných operačných systémoch implementované.

7.1 Bezpečnostný audit (FAU Security audit)

Operačné systémy Windows 95/98 neposkytujú žiadne prostriedky pre generovanie, zbieranie, ukladanie, prezeranie ani analýzy záznamov bezpečnostného auditu.

Operačný systém Linux negeneruje záznamy auditu na úrovni jadra systému (napr. prístup k objektom, nastavenie bezpečnostých atribútov a pod.). Na aplikačnej vrstve

[1] Aby sme boli korektní, tak Linux je jadro operačného systému. Používa sa spolu so sadou štandardných systémových aplikácií a knižníc, ktoré zabezpečujú aj niektoré bezpečnostné funkcie. Distribúcií operačných systémov založených na jadre Linux je viac (Slackware, Debian, RedHat, Mandrake, Suse, ...), no pre naše účely nie je potrebné ich rozlišovať. Podstatné bezpečnostné vlastnosti operačného systému založené na jadre Linux sú totiž určené práve týmto jadrom. Niektoré ďalšie bezpečnostné vlastnosti sú určené štandardnými systémovými aplikáciami a knižnicami, ktoré sa nachádzajú vo všetkých bežných distribúciach.

poskytuje štandardné rozhranie pre zber záznamov z aplikácií a umožňuje triedenie záznamov podľa kategórie aplikácie, ktorá ich vygenerovala a podľa závažnosti. Neposkytuje prostriedky automatickej analýzy záznamov auditu. Záznamy sa ukladajú do súborov a sú chránené prostriedkami riadenia prístupu. Môžu byť tiež posielané na iný server.

Operačné systémy Windows NT/2000/XP umožňujú generovanie záznamov auditu pre zvolené objekty a operácie s nimi. Taktiež umožňujú zber informácií z aplikácií. Poskytujú prostriedky na prezeranie záznamov auditu. Neposkytujú prostriedky automatickej analýzy záznamov auditu.

7.2 Komunikácia (FCO Communication)

Všetky tri skupiny operačných systémov sa štandardne distribuujú s prostriedkami, ktoré umožňujú aplikáciam používať kryptografické funkcie na vytváranie a overovanie dôkazov o pôvode informácie založených na digitálnych podpisoch. Využívanie týchto funkcií je však záležitosťou aplikácií.

Žiadny z uvažovaných operačných systémov nevytvára priamo dôkazy o doručení informácie. Realizácia týchto bezpečnostných funkcií je záležitosťou aplikácií.

7.3 Kryptografická podpora (FCS Cryptographic support)

Všetky tri skupiny operačných systémov sa štandardne distribuujú s prostriedkami, ktoré umožňujú aplikáciam generovanie kryptografických kľúčov pre bežne používané asymetrické a symetrické algoritmy. Operačné systémy Windows 2000 vo verzii Server a Linux sa bežne distribuujú aj s nástrojmi potrebnými na zabezpečenie bezpečnej distribúcie kľúčov na báze PKI[2] pomocou certifikátov verejných kľúčov.

Všetky tri skupiny operačných systémov sa štandardne distribuujú s prostriedkami, ktoré umožňujú aplikáciam vykonávanie štandardných kryptografických operácií. Podporované algoritmy sa môžu líšiť, no sú podporované všetky algoritmy bežne používané v štandardoch ako S/MIME alebo SSL.

7.4 Ochrana používateľských údajov (FDP User data protection)

7.4.1 Riadenie prístupu

Windows 95/98

Operačný systém Windows 95/98 neobsahuje žiadne funkcie riadenia prístupu pre lokálne subjekty, t.j. všetky subjekty (procesy) majú možnosť manipulovať s akýmikoľvek objek-

[2]Public Key Infrastructure – Infraštruktúra pre verejné kľúče

tami. Jediné funkcie riadenia prístupu, ktoré Windows 95/98 obsahujú, sú funkcie riadenia prístupu externých subjektov k zdieľaným zdrojom (najmä adresáre a tlačiarne) prostredníctvom počítačovej siete.

Linux

Subjektami operačného systému Linux, ktoré podliehajú riadeniu prístupu, sú procesy. Každý proces má priradený (efektívny) identifikátor používateľa, v mene ktorého práve vykonáva činnosť (effective user ID), (efektívny) identifikátor skupiny (effective group ID), v mene ktorej práve vykonáva činnosť, identifikátory doplnkových skupín, ktorých prístupové práva môže používať. Okrem týchto identifikátorov má priradené identifikátory používateľa (real user ID) a skupiny (real group ID), ktoré by mali predstavovať skutočnú identitu používateľa, ktorý proces spustil, a jeho primárnej skupiny. Tiež má priradený identifikátor používateľa (saved user ID) a skupiny (saved group ID), ktoré sa využívajú pri zmene efektívnych identifikátorov. Tieto identifikátory majú procesy aj v ostatných systémoch typu UNIX. Linux navyše procesom priraďuje ešte špeciálny identifikátor používateľa a skupiny, ktorý sa používa namiesto efektívneho pri riadení prístupu k objektom súborového systému, no tieto majú za normálnych okolností rovnakú hodnotu, ako príslušné efektívne identifikátory.

Objektami operačného systému Linux, ktoré podliehajú riadeniu prístupu, sú predovšetkým objekty súborového systému (súbory, adresáre, špeciálne súbory reprezentujúce zariadenia, pomenované rúry (pipe, FIFO) a zásuvky (sockets)), procesy, prostriedky medziprocesovej komunikácie typu System V.

Každý objekt súborového systému má priradený identifikátor používateľa – vlastníka, identifikátor skupiny a prístupové práva. Prístupové práva pozostávajú predovšetkým z troch trojbitových hodnôt, po jednej pre vlastníka, skupinu a ostatných. Jednotlivé bity reprezentujú práva na čítanie, zápis a spúšťanie súborov, resp. čítanie, zápis a použitie adresárov. Ak má proces požadujúci prístup hodnotu špeciálneho identifikátora používateľa rovnú identifikátoru vlastníka objektu, použijú sa prístupové práva pre vlastníka. Inak, ak je identifikátor skupiny objektu rovný špeciálnemu identifikátoru skupiny subjektu alebo je medzi identifikátormi doplnkových skupín subjektu, použijú sa práva pre skupinu. Inak sa použijú práva pre ostatných. Okrem týchto prístupových práv je pre adresáre definovaný bit, ktorý obmedzuje vymazanie a premenovanie objektu len na vlastníka objektu a vlastníka adresára aj v prípade, ak základné prístupové práva tak umožňujú spraviť aj inému subjektu. Pre súborové systémy, ktoré nepodporujú nastavovanie spomenutých prístupových práv a vlastníkov, sa tieto nastavujú globálne pre celý súborový systém pri jeho pripojení do systému. Navyše Linux umožňuje objektom súborových systémov, ktoré to podporujú[3], nastaviť príznaky *nezmeniteľný (immutable)*, ktorý zabraňuje zápisu, premenovaniu a vymazaniu objektu, a *len na pridávanie (append only)*, ktorý umožňuje zápis len na koniec súboru a tiež zabraňuje vymazaniu a premenovaniu súboru. Rozhodnutie o povolení prístupu subjektu k objektu sa riadi nasledovnými pravidlami podľa typu prístupu:

[3] napr. štandardné súborové systémy v Linux-e ext2 a ext3

- použitie cesty k objektu[4] – subjekt musí mať právo použiť všetky adresáre v ceste k objektu,
- otvorenie objektu na čítanie – subjekt musí mať právo čítať objekt,
- otvorenie objektu na zápis – subjekt musí mať právo zapisovať do objektu,
- vymazanie objektu – subjekt musí mať právo zápisu do adresára, odkiaľ chce objekt vymazať; ak má adresár nastavený bit obmedzujúci právo vymazať a premenovať objekty, musí byť špeciálny identifikátor používateľa subjektu rovný identifikátoru vlastníka objektu alebo adresára,
- premenovanie/presunutie objektu – subjekt musí mať právo zápisu do adresárov, odkiaľ a kam chce objekt presunúť; ak má zdrojový adresár nastavený bit obmedzujúci právo vymazať a premenovať objekty, musí byť špeciálny identifikátor používateľa subjektu rovný identifikátoru vlastníka objektu alebo tohto adresára,
- vytvorenie nového objektu – subjekt musí mať právo zápisu do adresára, v ktorom chce objekt vytvoriť[5],
- získať atribúty objektu – okrem použitia cesty k objektu nie sú ďalšie požiadavky,
- zmena prístupových práv objektu – subjekt musí mať špeciálny identifikátor používateľa rovný identifikátoru vlastníka objektu,
- zmena skupiny objektu – subjekt musí mať špeciálny identifikátor používateľa rovný identifikátoru vlastníka objektu a požadovaný nový identifikátor skupiny musí byť rovný špeciálnemu identifikátoru skupiny subjektu alebo musí byť medzi identifikátormi doplnkových skupín subjektu,
- zmena vlastníka objektu – subjekt musí mať špeciálne oprávnenie[6],
- zmena času poslednej modifikácie alebo prístupu k objektu na aktuálny čas – rovnaké požiadavky ako na zápis alebo špeciálny identifikátor subjektu rovný identifikátoru vlastníka objektu,
- zmena času poslednej modifikácie alebo prístupu k objektu na iný čas – špeciálny identifikátor subjektu musí byť rovný identifikátoru vlastníka objektu,
- nastavenie alebo zrušenie príznakov *nezmeniteľný* a *len na pridávanie* – subjekt musí mať špeciálne oprávnenie[6].

Explicitne je zakázané otvorenie na zápis, vymazanie, premenovanie objektu, zmena jeho atribútov (vlastník, skupina, práva, časy), ak sa objekt nachádza v súborovom systéme, ktorý je pripojený len na čítanie alebo má objekt nastavený príznak *nezmeniteľný*.

[4] Táto operácia je predpokladom ostatných.

[5] Linux umožňuje, aby jeden objekt bol prístupný vo viacerých adresároch alebo pod rôznymi menami. Sprístupnenie objektu na novom mieste má rovnaké požiadavky na práva ako vytvorenie nového objektu.

[6] Pri základnom nastavení systému má toto špeciálne oprávnenie každý proces, ktorého efektívny identifikátor používateľa je 0. To je identifikátor určený pre zvláštneho používateľa, štandardne nazývaného root, ktorý slúži predovšetkým na administráciu operačného systému a vykonávanie procesov, ktoré potrebujú špeciálne prístupové práva.

Otvorenie na zápis na iné miesto ako na koniec súboru, vymazanie a premenovanie objektu a zmena jeho vlastníka, skupiny alebo práv sú tiež zakázané, ak má objekt nastavený príznak *len na pridávanie*. V tejto súvislosti ešte treba podotknúť, že operácie vytvorenia, vymazania a premenovania objektu vo svojej podstate zahŕňajú zápis do príslušného adresára, takže ak je obmedzený zápis do príslušného adresára, nie je možné tieto operácie vykonať. Obmedzenia vyplývajúce z prístupových práv alebo požiadavky na zhodnosť identifikátora vlastníka alebo skupiny objektu so špeciálnym identifikátorom používateľa alebo skupiny subjektu sa nevzťahujú na subjekty so špeciálnymi oprávneniami[6].

Prostriedky medziprocesovej komunikácie typu System V (semafóry, zdieľané pamäťové segmenty a správy) majú, podobne ako objekty súborového systému, priradené identifikátory vlastníka a skupiny a navyše aj identifikátory používateľa a skupiny subjektu, ktorý ich vytvoril. Riadenie prístupu k prostriedkom medziprocesovej komunikácie typu System V je podobné riadeniu prístupu k objektom súborového systému.

Proces vystupuje aj v role objektu, keď mu iný proces posiela tzv. signál, alebo keď iný proces (subjekt) používa prostriedky na prístup do adresového priestoru procesu[7] (objektu). Riadenie prístupu k procesom je založené na princípe, že proces môže pristupovať len k procesu toho istého používateľa, ktorý nemá žiadne zvláštne prístupové práva. Výnimkou je prípad, keď subjekt má špeciálne oprávnenia[6].

Súhrnne možno konštatovať, že operačný systém Linux poskytuje prostriedky riadenia prístupu, ktoré umožňujú definovať prístupové práva pre vlastníka objektu, jednu skupinu používateľov a ostatných.

Windows NT/2000/XP

Subjektami operačného systému Windows NT/2000/XP sú procesy. Každý proces vykonáva operácie v mene nejakého používateľa (používateľmi pre tieto účely sú aj zvláštne systémové účty, ktoré slúžia na prevádzku rôznych služieb). Používatelia sú zaradení do skupín. Prístupové práva procesu sú určené prístupovými právami pridelenými používateľovi a skupinám, ktorých je členom.

Objektami podliehajúcimi riadeniu prístupu sú, podobne ako v operačnom systéme Linux, objekty súborového systému NTFS[8], zariadenia (napr. tlačiarne), zdieľané adresáre, procesy, zdieľaná pamäť a ďalšie objekty.

Riadenie prístupu k procesom zabraňuje manipulácii s procesmi iného používateľa. Výnimkou sú procesy patriace používateľovi, ktorý má špeciálne oprávnenia, ktoré môžu pristupovať k ľubovoľnému procesu.

Riadenie prístupu k objektom súborového systému, zdieľaným adresárom, zariadeniam a niektorým ďalším typom objektov je založené na použití zoznamov prístupových práv (Access control lists, ACL). Tieto je možné definovať pre každý objekt zvlášť a pri

[7] Linux využíva prostriedky hardvérovej vrstvy na oddelenie adresových priestorov jednotlivých procesov, takže procesy sa môžu navzájom ovplyvňovať výlučne použitím prostriedkov operačného systému.

[8] NTFS je štandardný súborový systém vo Windows NT/2000/XP. Pre súborové systémy typu FAT, ktoré nepodporujú prístupové práva, Windows NT/2000/XP neumožňujú riadenie prístupu.

objektoch súborového systému sa prístupové práva dedia z nadradeného adresára, ak nie je vo vlastnostiach objektu nastavené, že nemá práva dediť. Položky zoznamov prístupových práv obsahujú vždy prístupové práva pre určeného používateľa alebo skupinu. Základné prístupové práva pre objekty súborového systému sú:

Plný prístup (Full Control) – umožňuje všetky operácie s objektom

Meniť (Modify) – umožňuje plný prístup okrem zmeny prístupových práv, prevzatia vlastníctva a mazania podadresárov

Čítať a spúšťať (Read & Execute) – umožňuje prezeranie obsahu adresárov a súborov a spúšťanie programov, zisťovanie prístupových práv

Prezerať obsah adresárov (List Folder Contents) – dáva tú istú úroveň prístupu ako Čítať a spúšťať, ale vzťahuje sa len na adresáre

Čítať (Read) – umožňuje čítať obsah súborov a adresárov a zisťovať prístupové práva

Zapisovať (Write) – umožňuje vytvárať podadresáre a súbory, zapisovať do súborov a zisťovať prístupové práva

Tieto základné prístupové práva sú definované pomocou čiastkových prístupových práv, ktoré je možné prideľovať aj samostatne ako špeciálne práva:

Prechádzať adresáre/Spúšťať programy (Traverse Folder/Execute File) – pre adresáre určuje, či proces môže prechádzať adresárom, aby získal prístup k objektom v ňom alebo jeho podadresároch[9], pre súbory znamená oprávnenie spúšťať programy

Vypísať adresár/Čítať údaje (List Folder/Read Data) – umožňuje prezerať obsah adresára alebo súboru

Čítať atribúty (Read Attributes) – umožňuje čítať atribúty objektu určené súborovým systémom NTFS (napr. súbor len na čítanie, skrytý súbor, a pod.)

Čítať rozšírené atribúty (Read Extended Atributes) – umožňuje čítať aplikačne definované atribúty

Vytvárať súbory/Zapisovať údaje (Create Files/Write Data) – pre adresáre umožňuje vytvárať súbory, pre súbory umožňuje zapisovať údaje

Vytvárať adresáre/Pridávať údaje (Create Folders/Append Data) – pre adresáre umožňuje vytváranie podadresárov, pre súbory umožňuje pridávať údaje na koniec súboru

Zapisovať atribúty (Write Attributes) – umožňuje meniť atribúty objektu určené súborovým systémom NTFS

Zapisovať rozšírené atribúty (Write Extended Attributes) – umožňuje meniť aplikačne definované atribúty

[9] Používateľovi alebo skupine je možné globálne definovať oprávnenie nerešpektovať toto čiastkové právo. Štandardne je toto oprávnenie udelené skupine všetkých normálnych používateľov.

Mazať podadresáre a súbory (Delete Subfolders and Files) – umožňuje vymazanie podadresárov a súborov v adresári, aj ak na ne proces nemá právo Vymazať

Vymazať (Delete) – umožňuje vymazať objekt

Čítať práva (Read Permissions) – umožňuje čítať zoznam prístupových práv pre objekt

Meniť práva (Change Permissions) – umožňuje meniť zoznam prístupových práv, prístupové práva môže vždy meniť aj vlastník objektu

Prevziať vlastníctvo (Take Ownership) – umožňuje používateľovi prevziať vlastníctvo objektu, t.j. zmeniť vlastníka na seba alebo skupinu, ktorej je používateľ členom

Synchronizovať (Synchronize) – umožňuje procesu použiť objekt na synchronizáciu vlákien (thread-ov)

Vzťah základných a čiastkových prístupových práv je uvedený v tabuľke 7.1

Special Permissions	Full Control	Modify	Read & Execute	List Folder Contents	Read	Write
Traverse Folder / Execute File	x	x	x	x		
List Folder/Read Data	x	x	x	x	x	
Read Attributes	x	x	x	x	x	
Read Extended Attributes	x	x	x	x	x	
Create Files / Write Data	x	x				x
Create Folders / Append Data	x	x				x
Write Attributes	x	x				x
Write Extended Attributes	x	x				x
Delete Subfolders and Files	x					
Delete	x	x				
Read Permissions	x	x	x	x	x	x
Change Permissions	x					
Take Ownership	x					
Synchronize	x	x	x	x	x	x

Tabuľka 7.1: Prístupové práva v súborovom systéme NTFS

Riadenie prístupu k iným objektom podliehajúcim riadeniu prístupu je podobné. Prístupové práva sa nevzťahujú na procesy, ktorých používateľ (resp. niektorá z jeho skupín) má priradené zvláštne oprávnenie. Príkladom je zvláštne oprávnenie obchádzať

riadenie prístupu pridelené štandardne skupine určenej pre používateľov vykonávajúcich zálohovanie, alebo zvláštne oprávnenie na prevzatie vlastníctva objektu štandardne pridelené skupine Administrators. Zaujímavou črtou týchto operačných systémov je, že vlastníka súboru nemožno meniť ľubovoľne, ale proces s príslušným prístupovým právom alebo zvláštnym oprávnením ho môže zmeniť len na svojho používateľa alebo skupinu. Cieľom tohto opatrenia je zrejme zabrániť administrátorovi, aby prevzal vlastníctvo objektu, dočasne zmenil prístupové práva tak, aby mohol objekt čítať, následne zmenil prístupové práva a vlastníka späť, čím by zabránil pôvodnému vlastníkovi zistiť, že s objektom bolo manipulované. Toto opatrenie je však negované možnosťou obísť prístupové práva pre účely zálohovania a týmto spôsobom získať obsah súboru. Systémy Windows 2000 a XP poskytujú možnosť šifrovať súbory, avšak umožňujú globálne definovať používateľa, ktorý má možnosť rozšifrovať všetky zašifrované súbory.

Súhrnne možno konštatovať, že operačné systémy Windows NT/2000/XP poskytujú prostriedky riadenia prístupu, ktoré umožňujú pomerne presne definovať prístupové práva k objektom až na úroveň jednotlivých používateľov a skupín.

7.4.2 Zabezpečenie autentickosti údajov

Žiadny z uvažovaných operačných systémov neposkytuje na úrovni operačného systému digitálne podpisovanie uložených informácií. Všetky sa štandardne distribuujú s kryptografickými prostriedkami (viď časť 7.3), ktoré umožňujú aplikáciam digitálne podpisovanie informácií. Bežné distribúcie Linux-u obsahujú aplikácie umožňujúce digitálne podpisovanie a overovanie digitálnych podpisov. Operačné systémy Windows 2000 a XP umožňujú overovanie digitálnych podpisov na systémových komponentoch.

7.4.3 Ochrana zostatkovej informácie

Táto rodina požiadaviek sa týka ochrany informácie, ktorá zostala v pamäťových objektoch po ich uvoľnení. Operačné systémy Linux aj Windows NT/2000/XP vymazávajú informáciu uloženú vo voľných pamäťových stránkach pred ich pridelením procesu.

7.5 Identifikácia a autentifikácia

Systémy Windows 95/98 umožňujú, no nevyžadujú identifikáciu a autentifikáciu používateľa. Autentifikácia je štandardne riešená pomocou hesla. Systém je možné nastaviť tak, aby na identifikáciu a autentifikáciu využíval služby servera s Windows NT/2000/XP, Linux-om alebo iným operačným systémom, ktorý poskytuje potrebné sieťové služby. Keďže Windows 95/98 nepodporuje riadenie prístupu, identifikácia používateľa prakticky nemá vplyv na bezpečnosť – využíva sa napr. na uloženie nastavení prostredia a parametrov aplikácií zvlášť pre jednotlivých používateľov. Ak sa používa autentifikácia na základe lokálne overovaného hesla, ktorýkoľvek používateľ má možnosť vymazať súbor s informáciami na overenie hesla iného používateľa a následne mu definovať iné heslo.

Systémy Windows NT/2000/XP štandardne požadujú identifikáciu a autentifikáciu používateľa pred tým, ako mu umožnia vykonávať iné činnosti so systémom[10]. Autentifikácia je štandardne riešená pomocou hesla, ktoré je overované lokálne alebo sa využívajú služby iného servera s operačným systémom Windows NT/2000/XP, Linux alebo iným, ktorý poskytuje potrebné sieťové služby. Systémy Windows NT/2000/XP umožňujú riešiť autentifikáciu aj inými prostriedkami, napr. použitím kryptografických čipových kariet, pomocou pridaných komponentov. Identifikácia používateľa sa prenáša na procesy, ktoré používateľ spustí, a využíva sa na prideľovanie prístupových práv.

Systém Linux štandardne vyžaduje identifikáciu a autentifikáciu používateľa pred tým, ako mu umožní vykonať iné činnosti[11]. Autentifikácia je štandardne riešená pomocou hesla, ktoré je overované lokálne alebo využitím služieb servera poskytujúceho niektoré z podporovaných autentifikačných služieb. V mnohých distribúciach je autentifikácia riešená modulárne a je možné pridávať moduly podporujúce iné metódy autentifikácie. Pri vzdialenom prístupe sa často využíva protokol *ssh*, ktorý umožňuje aj autentifikáciu založenú na digitálnych podpisoch. Identifikácia používateľa sa využíva na nastavenie identifikátorov používateľa a skupín procesom, ktoré používateľ spustí.

7.6 Správa bezpečnosti (FMT Security management)

Táto trieda požiadaviek sa týka manipulácie s bezpečnostnými atribútmi (napr. identifikátory používateľa priradené procesu), údajmi bezpečnostných funkcií (napr. heslá, konfigurácia systému) a používania špeciálnych funkcií, ktoré majú globálny dopad na funkciu alebo bezpečnosť systému.

Linux

Procesy majú priradené bezpečnostné atribúty (napr. identifikátory používateľa a skupiny, priorita, limity na využívanie systémových zdrojov a pod.). Proces môže tieto parametre meniť len vtedy, ak má špeciálne oprávnenie[6], alebo ak zmena nemôže mať negatívny dopad na zvyšok systému. Zvláštnu pozornosť si zaslúžia identifikátory používateľa. Tie môže proces bez špeciálneho oprávnenia nastaviť len na hodnotu, ktorú má niektorý z týchto identifikátorov. Linux umožňuje nastaviť spúšťateľnému súboru príznak, že proces, ktorý vznikne jeho spustením, má mať nastavený efektívny identifikátor používateľa (a zároveň aj saved user ID a špeciálny identifikátor pre riadenie prístupu k súborom) na vlastníka súboru. To sa využíva pre programy, ktoré majú byť schopní spustiť bežní používatelia, ale ktoré potrebujú vykonávať činnosti s inými prístupovými právami. Takýto proces potom môže prepínať svoj efektívny identifikátor používateľa medzi reálnym identifikátorom používateľa a saved user ID. Podobný mechanizmus existuje aj pre identifikátory skupín.

[10] Štandardne je možné pred identifikáciou a autentifikáciou používateľa ukončiť prácu systému alebo reštartovať počítač, no je možné to zakázať.

[11] V prípade fyzického prístupu ku klávesnici počítača môže používateľ zvyčajne vykonať reštart alebo vypnutie systému, ale je možné to zakázať alebo zmeniť na ľubovoľnú inú akciu.

Nastavovaniu bezpečnostných atribútov objektom (napr. prístupové práva, vlastník, skupina) sme sa venovali pri popise funkcií na riadenie prístupu v časti 7.4.1.

Mnohé informácie používané bezpečnostnými funkciami (napr. informácie na overovanie hesiel) sú uložené v súboroch. Prístup k nim je chránený prostriedkami riadenia prístupu, pričom sa využíva vyššie uvedená možnosť spúšťať vybrané programy s iným efektívnym identifikátorom používateľa ako je používateľ, ktorý program spustí (napr. program na zmenu hesla používateľa tak získa potrebné prístupové práva na zápis do databázy informácií na overovanie hesiel a môže heslo zmeniť).

Nastavovať rôzne parametre systému a používať funkcie, ktoré majú zásadný vplyv na systém a ostatné procesy, môžu len procesy so špeciálynmi oprávneniami. Týchto špeciálnych oprávnení je 29. Štandardné jadro Linux-u všetky tieto oprávnenia pridelí procesu, ktorý má efektívny identifikátor používateľa 0. Procesu, ktorý má iný efektívny identifikátor používateľa, nepridelí žiadne z týchto oprávnení. Takéto správanie je kompatibilné s bežnými systémami typu UNIX. Proces však môže svoje oprávnenia trvale alebo dočasne znížiť a obmedziť tak prípadné nežiadúce účinky, napr. následkom chyby v programe. V súčasnosti sa však tieto možnosti využívajú zriedkavo.

Windows 95/98

Operačné systémy Windows 95/98 neposkytujú žiadne prostriedky manažmentu bezpečnostných atribútov, údajov ani špeciálnych funkcií. Každý proces k nim má nekontrolovaný prístup.

Windows NT/2000/XP

Operačné systémy Windows NT/2000/XP umožňujú priradiť používateľom a skupinám niekoľko[12] zvláštnych oprávnení, ktoré umožňujú obchádzať niektoré prístupové práva, vykonávať činnosti so zásadným vplyvom na funkčnosť alebo bezpečnosť systému, alebo využívať niektoré služby systému. Zvyčajne sa tieto zvláštne oprávnenia prideľujú skupinám, a tým všetkým používateľom, ktorí sú členmi týchto skupín.

Rôzne informácie používané bezpečnostnými funkciami sú uložené v súboroch, ku ktorým systém umožňuje prístup len prostredníctvom príslušných bezpečnostných funkcií.

7.7 Ochrana súkromia (FPR Privacy)

Žiadny z uvažovaných operačných systémov neobsahuje bezpečnostné funkcie spĺňajúce požiadavky tejto triedy, ktoré sú zamerané na nemožnosť zistenia identity používateľa zodpovedného za daný proces.

[12] vo Windows XP 37

7.8 Ochrana bezpečnostných funkcií (FPT Protection of security functions)

Všetky tri skupiny operačných systémov využívajú prostriedky hardvérovej vrstvy na ochranu pamäte operačného systému pred manipuláciou procesmi a ochranu pamäte procesov pred priamou manipuláciou inými procesmi. V operačných systémoch Windows NT/2000/XP a Linux sú systémové súbory chránené riadením prístupu.

7.9 Využívanie zdrojov (FRU Resource utilisation)

Operačný systém Linux priraďuje každému procesu prioritu, podľa ktorej sa riadi prideľovanie procesorového času procesom. Proces bez špeciálnych oprávnení[6] môže svoju prioritu len znižovať. Linux ďalej umožňuje obmedziť maximálne množstvo spotrebovaných systémových zdrojov (napr. pamäť, počet súborov, procesorový čas) jedným procesom a maximálny počet procesov patriacich jednému používateľovi. Linux tiež umožňuje nastaviť obmedzenia na počet súborov a celkovú veľkosť spotrebovaného diskového priestoru pre jedného používateľa alebo skupinu používateľov. Linux poskytuje aj prostriedky na zvýšenie odolnosti systému proti zlyhaniu diskov – umožňuje niekoľko diskov skombinovať do redundantného diskového poľa[13].

Operačné systémy Windows NT/2000/XP umožňujú tiež definovať procesom priority, na základe ktorých sa riadi prideľovanie procesorového času. Tiež je možné definovať obmedzenia na veľkosť pamäte spotrebovanej procesom. Na nastavovanie týchto obmedzení spôsobom, ktorý má negatívny dopad na ostatné procesy, je potrebné zvláštne oprávnenie. Operačný systém Windows XP umožňuje definovať obmedzenie na spotrebu diskového priestoru jednotlivým používateľom.

7.10 Prístup k systému (FTA Access)

Operačné systémy Windows 95/98 ani Windows NT/2000/XP štandardne neinformujú používateľa o čase posledného prihlásenia k systému. Operačné systémy Windows NT/2000/XP umožňujú používateľovi uzamknúť konzolu[14], čím dôjde k prekrytiu obrazu a znemožní sa ďalšia práca bez novej autentifikácie používateľa. K uzamknutiu konzoly môže dôjsť aj automaticky po určitom čase neaktivity používateľa.

Operačný systém Linux štandardne pri prihlásení používateľa na textovej konzole informuje o čase a mieste posledného prihlásenia a počte predchádzajúcich neúspešných pokusov o prihlásenie. Všetky bežné grafické prostredia pre Linux umožňujú uzamknúť grafickú konzolu, čím dôjde k prekrytiu obrazu a znemožní sa ďalšia interakcia s používateľovými aplikáciami bez novej autentifikácie. K uzamknutiu môže dôjsť aj automaticky po určitom čase neaktivity používateľa.

[13] Linux podporuje režimy RAID 0, 1, 4, 5 a umožňuje ich navzájom kombinovať.
[14] Pod pojmom konzola rozumieme klávesnicu a obrazovku.

7.11 Dôveryhodná cesta a kanál (FTP Trusted path / channel)

Operačné systémy Windows 95/98 neposkytujú dôveryhodnú cestu medzi funkciami operačného systému a používateľom.

Operačné systémy Windows NT/2000/XP poskytujú dôveryhodnú cestu pre komunikáciu používateľa so systémom pri zadávaní identifikačných a autentifikačných údajov. Tieto systémy definujú jednu kombináciu klávesov, na ktorú nemôžu reagovať aplikačné programy, čím používateľ získa istotu, že po jej použití komunikuje s procesom definovaným operačným systémom a nie nejakým procesom iného používateľa, ktorý sa graficky prezentuje rovnako.

Operačný systém Linux tiež poskytuje dôveryhodnú cestu medzi používateľom prítomným pri klávesnici počítača a programom na úvodnú identifikáciu a autentifikáciu používateľa. Umožňuje definovať kombináciu klávesov, ktorých stlačenie nemôže byť monitorované žiadnym aplikačným programom a má za následok zrušenie všetkých procesov, ktoré čítajú klávesnicu. Následne sa spustí program na identifikáciu a autentifikáciu používateľa, ktorý má istotu, že komunikuje s programom definovaným administrátorom systému a nie programom iného používateľa, ktorý sa rovnako prezentuje. Pri vzdialenom prihlasovaní sa použitím protokolu ssh je poskytovaný dôveryhodný komunikačný kanál medzi stanicou používateľa a počítačom, ku ktorému sa používateľ prihlasuje. Ochrana komunikačného kanála je zabezpečená kryptografickými prostriedkami. Zabezpečená je dôvernosť aj integrita prenášaných údajov a autentifikácia servera aj používateľa.

Kapitola 8

Zhrnutie bezpečnostných funkcií bežných operačných systémov

Bežné operačné systémy, ktorým sme sa venovali v predchádzajúcej kapitole, môžeme z hľadiska bezpečnosti rozdeliť na dve skupiny. Jednu tvoria systémy Windows 95/98, ktoré neposkytujú riadenie prístupu k používateľským údajom a aplikáciam, a ktoré ani nezabezpečujú dostatočnú ochranu operačného systému. Tieto operačné systémy nie sú použiteľné na ukladanie ani spracovanie informácií, ktorých bezpečnosť je potrebné chrániť. Jedinou možnosťou je použitie takéhoto systému jediným používateľom a adekvátna fyzická ochrana počítača, na ktorom je prevádzkovaný. Navyše, ako uvidíme ďalej, takýto systém musí byť používaný len na vymedzené účely, pri ktorých je nízke riziko inštalácie alebo spustenia softvéru s neznámymi vedľajšími účinkami. Ak by sme tieto systémy mali hodnotiť z hľadiska naplnenia funkčných požiadaviek podľa kritérií TCSEC, tieto systémy by boli v triede D.

Druhú skupinu tvoria operačné systémy Linux a Windows NT/2000/XP. Tieto operačné systémy poskytujú separáciu informácií a procesov podľa používateľov a ich skupín a zabezpečujú voliteľnú ochranu[1] objektov prostriedkami riadenia prístupu. Podľa funkčných kritérií TCSEC by tieto systémy patrili do triedy C. Tieto operačné systémy sú použiteľné na ukladanie a spracovanie informácií s požiadavkami na bezpečnosť s určitými obmedzeniami. Závažnosť týchto obmedzení závisí od konkrétnych okolností. V nasledujúcich častiach sa budeme venovať najzávažnejším problémom, ktoré obmedzujú použiteľnosť týchto operačných systémov na spracovanie bezpečnostne citlivých informácií.

8.1 Zneužitie prístupových práv administrátorom systému

V operačnom systéme Linux sa na používateľa s identifikátorom 0 (štandardne nazývaného root) nevzťahujú obmedzenia riadenia prístupu. Administrátor systému má typicky možnosť spúšťať akékoľvek procesy v mene používateľa root. Týmto spôsobom môže nielen ľubovoľne manipulovať so všetkými údajmi používateľov, ale napr. aj mod-

[1] Voliteľná ochrana je ochrana závislá od rozhodnutia používateľa, ktorý informáciu vytvoril.

ifikovať aplikácie a súčasti operačného systému tak, aby sledovali dôverné vstupy od používateľa (napr. heslá, PIN).

V operačných systémoch Windows NT/2000/XP majú používatelia možnosť obmedziť prístup administrátorov k svojim údajom. Ako sme však uviedli v časti 7.4.1, táto možnosť nie je dostatočne účinná, pretože je možné tieto prístupové práva obísť využitím zvláštnych oprávnení pre zálohovanie. Dôvernosť údajov je možné zvýšiť použitím šifrovania, ktoré systémy ponúkajú, no ak je v systéme definovaný aj používateľ, ktorý má byť schopný rozšifrovať súbory iných používateľov bez znalosti ich hesla, nie je ani táto ochrana dostatočná.

Tieto skutočnosti dávajú administrátorm (a prípadne iným používateľom so zvláštnymi oprávneniami) veľkú kontrolu nad celým systémom. Preto je veľmi dôležitá dôveryhodnosť osôb, ktoré sú administrátormi a inými privilegovanými používateľmi.

8.2 Veľa procesov s vysokými prístupovými právami

Ďalším veľmi častým problémom je, že mnohé procesy zabezpečujúce rôzne služby sú spúšťané v mene privilegovaných používateľov. Mnohé takéto programy ich prístupové práva a iné oprávnenia potrebujú, no časté sú aj prípady, že z nich potrebujú len časť. V programoch sa často vyskytujú rôzne chyby, ktoré umožňujú útočníkom vykonať ľubovoľný kód s právami napadnutého procesu. Keď takúto chybu obsahuje program bežiaci v mene administrátora, chyby v ňom umožňujú zneužitie prístupových práv administrátora aj iným subjektom – často neidentifikovateľným externým útočníkom.

8.3 Zneužitie prístupových práv používateľa

V súčasnosti veľmi aktuálnym bezpečnostným problémom je zneužívanie práv používateľa programami z neznámych zdrojov. Dochádza k nemu najmä dvomi spôsobmi. Jedným je využitie nevedomosti používateľov, ktorí si často neuvedomujú, že programy, ktoré získali z rôznych zdrojov (napr. z Internetu), môžu okrem (alebo namiesto) svojej deklarovanej činnosti vykonávať aj iné operácie, pričom disponujú všetkými prístupovými právami, ktoré používateľ má.

Druhým veľmi bežným problémom sú chyby v aplikáciach, ktoré umožňujú pri spracovaní vhodne vytvoreného dokumentu vykonať ľubovoľný programový kód obsiahnutý v dokumente. Keď používateľ použije takúto aplikáciu na spracovanie dokumentu z neznámeho zdroja, vystavuje sa podobnému riziku, ako pri spustení programu z neznámeho zdroja. S týmto problémom súvisia vlastnosti niektorých programov – napr. prehliadačov WWW stránok alebo elektronickej pošty, ktoré v snahe uľahčiť a spríjemniť prácu používateľovi, umožňujú automatické spúšťanie aplikácií na spracovanie vložených dokumentov, často aj skôr ako má používateľ možnosť rozhodnúť sa, či dokument otvoriť chce alebo nie. To je v súčasnosti asi najrozšírenejší spôsob šírenia počítačových vírusov a trójskych koní. Využívaniu tohto spôsobu zneužívania prístupových práv používateľa značne napomáha aj nevedomosť používateľov a ich dôverčivosť voči informáciam, ktoré

nepochádzajú z dôveryhodných zdrojov. Typickým príkladom sú adresy odosielateľa elektronickej pošty, ktoré je veľmi ľahké falšovať, čo sa aj v značnej miere využíva. Používatelia potom často veria, že správu dostali od človeka, ktorého poznajú, a ktorému dôverujú, no v skutočnosti správa pochádza od vírusu, ktorý sa snaží využiť bezpečnostnú dieru v niektorom programe, ktorý používateľ použije na zobrazenie správy.

8.4 Manipulácia s hardvérom

Nezanedbateľná možnosť narušenia bezpečnosti spomínaných operačných systémov je manipulácia s hardvérom v čase, keď nie je pod kontrolou operačného systému. Ak má útočník fyzický prístup k počítaču, môže modifikovať obsah jeho disku a týmto spôsobom zmeniť ľubovoľné údaje, aplikácie alebo časti operačného systému. Operačné systémy Windows 2000 a XP umožňujú overovať digitálne podpisy systémových komponentov, no na ich overovanie používajú informácie uložené tiež na disku, ktoré sú preto tiež vystavené riziku modifikácie. Tiež nie je vylúčená možnosť modifikácie príslušnej časti operačného systému, aby digitálne podpisy nekontroloval. Tieto problémy nie je vo všeobecnosti možné riešiť na úrovni operačného systému inak ako spúšťaním systému z nemodifikovateľného pamäťového média, ktorého fyzická ochrana je primerane zabezpečená.

8.5 Čiastočné riešenia

Niektoré vyššie uvedené problémy je možné čiastočne riešiť aj prostriedkami poskytovanými operačnými systémami Linux a Windows NT/2000/XP. Problémy s procesmi s vysokými prístupovými právami je niekedy možné riešiť obmedzením prístupových práv alebo zvláštnych oprávnení na najnižšiu možnú úroveň, ktorá je potrebná pre činnosť procesu. To však často nie je postačujúce alebo možné.

Problémy so zneužívaním prístupových práv používateľov sa dajú čiastočne riešiť vzdelávaním používateľov a striktným oddelením rizikových činností a činností s prístupom k citlivým údajom. Keď bude používateľ na tieto skupiny činností používať rozdielne používateľské kontá, je možné nastaviť prístupové práva tak, aby programy spustené v mene konta pre rizikové činnosti (prezeranie WWW a elektronickej pošty, spúšťanie programov pochybného pôvodu a pod.) nemali prístup k citlivým údajom, ku ktorým majú prístup len procesy spustené v mene druhého konta.

Pre operačný systém Linux vzniklo niekoľko projektov (napr. [16, 19, 20, 15, 18]), ktorých cieľom bolo implementovať rôzne bezpečnostné mechanizmy (najmä prostriedky povinnej ochrany typické pre systémy triedy B podľa TCSEC), ktoré umožňujú efektívne riešiť niektoré zo spomínaných bezpečnostných problémov. Tieto riešenia modifikovali jadro systému, takže bolo potrebné ich prispôsobovať novým verziám jadra. Následne boli vedené diskusie o tom, ktorý z týchto projektov je univerzálnym riešením, ktoré by sa mohlo stať štandardnou súčasťou jadra Linux-u. Žiadny z projektov nebol zvolený, pretože nebolo možné určiť, že jeden je "ten pravý", no vznikol medzinárodný projekt

špecifikácie rozhrania pre implementáciu bezpečnostných rozšírení Linux-u – Linux Security Modules (LSM) [17]. Prispievateľmi do tohto projektu boli aj mnohí autori existujúcich rozšírení a výsledkom je špecifikácia, ktorá by sa mala stať oficiálnou súčasťou jadra Linux-u. Toto rozhranie by malo umožniť implementovať bezpečnostné rozšírenia Linux-u ako moduly, ktoré budú využívať dobre definované rozhranie, a vďaka tomu ich nebude nutné často prispôsobovať vývoju jadra. Niektoré z pôvodných bezpečnostných rozšírení už boli implementované ako moduly podľa špecifikácie LSM.

Časť III

Bezpečnosť vo vývoji a prevádzke IKT systémov

Kapitola 9

Údržba softvéru

Neoddeliteľnou súčasťou udržiavania bezpečnosti IKT systému je jeho údržba. V priebehu prevádzky IKT systému dochádza k odhaľovaniu rôznych chýb, či už v návrhu alebo v implementácii jeho softvérových alebo aj hardvérových. Chyby môžu mať dopad na funkčnosť aj bezpečnosť IKT systému. Chyby s dopadom na bezpečnosť sa zvyčajne veľmi rýchlo stanú verejne známymi, preto je potrebné, aby boli včas dostupné aj ich opravy.

V prípade proprietárneho softvéru je používateľ zvyčajne odkázaný na tvorcu softvéru. V licenčných zmluvách sa tvorcovia proprietárneho softvéru zvyčajne v maximálnej možnej miere zbavujú právnej zodpovednosti za prípadné škody, ktoré vzniknú používaním ich softvéru a neposkytujú právne vymáhateľné záruky za včasnú tvorbu a poskytovanie opráv v prípade odhalenia bezpečnostných chýb. Je však bežné, že počas určitej obmedzenej doby reagujú na odhalenia chýb a opravy na svoje produkty vytvárajú a zákazníkom poskytujú. V niektorých prípadoch sú opravy k dispozícii v priebehu niekoľkých dní, v niektorých sú tieto časy podstatne dlhšie. Problémom je však údržba starších, už nepodporovaných produktov alebo ich verzií. Zákazník je v takých prípadoch nútený investovať do prechodu na nové verzie alebo riskovať bezpečnostné incidenty. Prechod na nové verzie môže okrem nových investícií znamenať aj problémy s kompatibilitou s ostatnými časťami IKT systému. Preto výmena jedného komponentu často vedie k núteným výmenám ďalších komponentov.

Jednou z častých výhrad proti Open Source softvéru je tvrdenie, že neexistuje subjekt zodpovedný za jeho vývoj a údržbu, a že preto aj chýbajú záruky za tvorbu opráv. Ako sme však uviedli v predchádzajúcom odseku, takéto záruky nie sú bežné ani u proprietárneho softvéru. Bežná prax však ukazuje, že vážnych (napr. bezpečnostných) chýb sú odhalených v Open Source softvéri sú zvyčajne k dispozícii v priebehu niekoľkých hodín, maximálne niekoľkých dní. Je pravdou, že podobne ako u proprietárneho softvéru, aj u Open Source softvéru býva podporovaný len obmedzený počet verzií. Avšak narozdiel od proprietárneho softvéru, prechody na novšie verzie neznamenajú náklady na nákup nových licencií. Veľký rozdiel je však v prípade, keď prechod na inú verziu z nejakých dôvodov nie je možný, alebo sa nejaký softvér prestal vyvíjať. Vďaka dostupnosti zdrojového kódu je totiž možné, aby odhalené chyby opravil aj niekto iný ako pôvodný tvorca softvéru.

Literatúra

[1] *An Introduction to Computer Security. The NIST Handbook.*, volume 800-12 of *NIST Special Publication*. NIST, 1996.

[2] *Common Methodology for Information Technology Security Evaluation, Introduction and General Model*, volume 1 of *CEM 97/017*. ISO/IEC, 1997.

[3] *International Standard ISO/IEC 15408 Common Criteria for Information Technology Security Evaluation. Annexes*, volume 2a. ISO/IEC, 1998.

[4] *International Standard ISO/IEC 15408 Common Criteria for Information Technology Security Evaluation. Introduction and General Model*, volume 1. ISO/IEC, 1998.

[5] *International Standard ISO/IEC 15408 Common Criteria for Information Technology Security Evaluation, Security Assurance Requirements*, volume 3. ISO/IEC, 1998.

[6] *International Standard ISO/IEC 15408 Common Criteria for Information Technology Security Evaluation. Security Functional Requirements*, volume 2. ISO/IEC, 1998.

[7] *Common Methodology for Information Technology Security Evaluation, Evaluation Methodology*, volume 2 of *CEM 99/045*. ISO/IEC, 1999.

[8] *International Standard ISO/IEC 17799, Information technology - Code of practice for information security management,*. ISO/IEC, 2000.

[9] *IT-Grundschutzhandbuch 2002, Maßnahmenemplehlungen für den mittleren Schutzbedarf*. BSI, 2002.

[10] *Standards for Security Categorization of Federal Information and Information Systems*. FIPS PUB. NIST, 2003.

[11] Grance T., Kent K., and Kim B. *Draft Computer Security Incident Handling Guide*, volume 800-61 of *NIST Special Publication*. NIST, 2003.

[12] Swanson M. *Guide for Developing Security Plans for Information Technology Systems*, volume 800-18 of *NIST Special Publication*. NIST, 1998.

[13] Stoneburner G., Goguen A., and Feringa A. *Risk Management Guide for Information Technology Systems. Recommendations of the National Institute of Standards and Technology*, volume 800-30 of *NIST Special Publication*. NIST, 2001.

[14] Swanson M. and Guttman B. *Generally Accepted Principles and Practices for Securing Information Technology Systems*, volume 800-14 of *NIST Special Publication*. NIST, 1996.

[15] *Domain and Type Enforcement*. `http://www.cs.wm.edu/~hallyn/dte/`.

[16] *Linux Intrusion Detection System*. `http://www.lids.org/`.

[17] *Linux Security Modules*.
texttthttp://lsm.immunix.org/.

[18] *Medusa DS9*. `http://medusa.fornax.sk/`.

[19] *Role Set Based Access Control*. `http://www.rsbac.org/`.

[20] *Security Enhanced Linux*. `http://www.nsa.gov/selinux/`.

Časť IV

Dodatky

Kapitola 10

Stručný výkladový slovník bezpečnostných termínov

Výkladový slovník obsahuje najdôležitejšie pojmy, s ktorými sa v dokumente pracuje, resp. ktoré sú potrebné pri tvorbe bezpečnostného modelu systému.

Access (prístup) (1) špecifický typ interakcie medzi subjektom a objektom, ktorého výsledkom je tok informácií od jedného k druhému. (2) Schopnosť a prostriedky potrebné na dosiahnutie, uloženie alebo získanie údajov; na komunikáciu s alebo použitie nejakého zdroja IKT systému.

Access control (riadenie prístupu) (1) Ohraničenie práv alebo možností subjektu komunikovať s inými subjektami alebo používať funkcie alebo služby IKT systému. (2) Obmedzenia riadiace prístup subjektu k objektu.

Access right (prístupové právo) Povolenie uskutočňovať nejaký typ prístupu (access type) udelené subjektu alebo objektu

Access type (typ prístupu) špecifický typ interakcie ktorý možno uplatniť na nejakom objekte

Accountability (zodpovednosť) vlastnosť alebo stav IKT systému umožňujúca priradiť činnosti uskutočnované v systéme jednotlivcom, ktorých potom možno za ne brať na zodpovednost. Činnosti zahrnajú porušenia a pokusy o porušenia bezpečnostnej politiky ako aj povolené činnosti.

Administrator (administrátor) osoba, ktorá je v kontakte s IKT systémom a je zodpovedná za udržiavanie jeho operačných schopností

Assurance (záruka) Stupeň dôvery v to, že IKT systém adekvátne splna bezpečnostné požiadavky. Dva hlavné aspekty záruk sú efektívnosť a korektnosť.

Assurance level (úrovenň záruk) preddefinovaná množina komponentov záruk, ktorá priraďuje mieru vlastnej bezpečnostnej kvality IKT systému. Ak IKT systém dosahuje nejakú úroveň záruk, znamená to že sa na IKT systém použili všetky prostriedky záruk (assurace measures) prislúchajúce danej úrovni.

Attack (útok) Pokus o obídenie bezpečnostných mechanizmov IKT systému. Môže byť aktívny (narušenie údajov) alebo pasívny (získanie údajov).

Audit (audit) Nezávislé skúmanie a vyhodnotenie záznamov a aktivít za účelom určenia súladu s definovnými pravidlami a zistenia prípadných nedostatkov v bezpečnostnej politike IKT systému alebo jej uplatnovaní.

Autentication (autentifikcia) (1) Overenie identity používateľa, zariadenia alebo inej entity. (2) Overenie integrity uložených, prenášaných údajov, alebo údajov iným spôsobom vystavených možnosti neoprávnenej modifikácie v IKT systéme.

Autorization (autorizácia) Udelenie prístupových práv pre používateľa, program alebo proces.

Availability (dostupnosť) Požiadavka, aby informácia a iné zdroje systému boli prístupné oprávneným používateľom bez zbytočného zdržiavania vtedy, keď to je potrebné.

Certification (certifikácia) vyčerpávajúca evaluácia technických a netechnických bezpečnostných rysov systému, ktorá sa robí ako častť, alebo na podporu procesu schvaľovania/akreditácie; ktorá stanovuje rozsah v ktorom sa konkrétny návrh a implementácia zhoduje so zadanou množinou bezpečnostných požiadaviek

Channel (kanál) cesta v systéme slúžiaca na prenos údajov. Môže tiež predstavovať mechanizmus, prostredníctvom ktorého sa cesta realizuje.

Compromise (kompromitácia) narušenie bezpečnosti systému, ktoré môže viesť k odhaleniu citlivej iformácie

Confidentiality (dôvernosť) Bezpečnostný atribút vyjadrujúci to, že obsah správy, údajov nie je odhalený nepovolanej osobe, procesu, entite alebo organizácii.

Configuration (konfigurácia) výber jednej z možných kombinácií parametrov systému

Configuration control (riadenie konfigurácie) manažment zmien hardvéru, softvéru, firmvéru a dokumentácie systému v priebehu jeho vývoja a celého životného cyklu

Configuration management (manažment konfigurácie) Manažment bezpečnostných charakteristík a záruk systému prostredníctvom zmien hardvéru, softvéru, firmvéru, dokumentácie, testov a ich dokumentácie v priebehu vývoja a životného cyklu systému.

Contingency plan (plán na zachovanie kontinuity činnosti) Plán reakcií na mimoriadne situácie, operácie zálohovania a obnovy systému po havárii, ktorý je súčastou bezpečnostného programu organizácie. Jeho cieľom je zaistiť dostupnosť kritických zdrojov a umožniť kontinuitu operácií systému v núdzových situáciách.

Cost-risk analysis (analýza rizík a nákladov) Odhad nákladov na ochranu údajov v systéme v porovnaní s ujmou spôsobenou stratou alebo kompromitáciou údajov.

Countermeasure (protiopatrenie) Činnosť, zariadenie, procedúra, technika alebo iný prostriedok, ktorý redukuje zraniteľnosť systému nejakou hrozbou.

Covert Channel (skrytý kanál) Komunikačný kanál, ktorý umožnuje nejakému pro-

cesu prenášať informácie spôsobom, ktorá je v rozpore s bezpečnostnou politikou systému

Data (údaje) Informácia v špecifickej fyzickej reprezentácii.

Data confidentiality (dôvernosť údajov) bezpečnostný atribút údajov, ktorý vyjadruje, že údaje sú chránené pred neoprávneným odhalením.

Data Integrity (integrita údajov) bezpečnostný atribút údajov, ktorý vyjadruje, že údaje sú chránené pred neoprávnenou modifikáciou alebo zničením.

Data security (bezpečnosť údajov) ochrana údajov pred neoprávnenou (neúmyselnou alebo zámernou) modifikáciou, zničením alebo odhalením.

Denial of service (odmietnutie služby) zabránenie autorizovanému prístupu k nejakej položke alebo službe systému, alebo oneskorenie časovo kritickej operácie

Environment (prostredie) všetko (používatelia, procedúry, objekty, podmienky, iné systémy), čo má vplyv na systém

Evaluation (evaluácia) technické posúdenie vlastností skúmaného systému, ktorého cieľom je určiť, či skúmaný systém vyhovuje stanoveným požiadavkám

Formal (formálny) založený na jednoznačnej syntaxi a sémantike

Formal proof (formálny dôkaz) matematický dôkaz

Formal Security Policy Model (formálny model bezpečnostnej politiky) Matematicky presná formulácia bezpečnostnej politiky. Aby bol dstatočne presný, takýto model musí reprezentovať počiatočný stav systému, spôsob, akým systém prechádza z jedného stavu do druhého a definíciu "bezpečného" stavu systému. Musí sa dať formálne dokázať, že ak požiatočný stav systému vyhovuje definícii bezpečného stavu a ak sú všetky požiadavky, ktoré model vyžaduje splnené, tak potom budú aj všetky nasledujúce stavy systému bezpečné.

Formal specification (formálna špecifikácia) popis systému používajúci obmedzenú syntax a gramatiku formálneho logického systému a množinu termínov, ktoré boli presne definované alebo špecifikované

Formal verification (formálna verifikácia) proces použíajúci formálne dôkazy na demonštráciu konzistencie (verifikácia návrhu) medzi formálnou špecifikáciou systému a formálnym modelom bezpečnostnej politiky alebo medzi formálnou špecifikáciou a implementáciou systému (verifikácia implementácie).

Functional testing (funkcionálne testovanie) časť bezpečnostného testovania, pri ktorom sa deklarované rysy systému testujú na korektnosť operácií

Functionality (funkcionalita) množina funkcionálnych bezpečnostnych požiadaviek, ktorá sa má implementovať v IKT systéme

Granularity (granularita) rozlišovacia úroveň, na ktorú možno nejaký mechanizmus nastaviť

Identification (identifikácia) proces ktorý umožnuje IKT systému rozpoznať nejakú entitu

Implementation (implementácia) fáza vývojového procesu systému, v ktorej sa detailná špecifikácia systému realizuje pomocou hardvéru a softvéru

Individual accountability (individuálna zodpovednosť) schopnosť systému spojiť identitu používatela s časom, metódou a stupnom prístupu k systému

Informal (neformálny) vyjadrený v prirodzenom jazyku

Informal specification (neformálna špecifikácia) popis/špecifikácia systému v prirodzenom jazyku

Least privilege (najmenšie privilégium) princíp, ktorý vyžaduje, aby každý subjekt dostal najmenšie možné oprávnenia, ktoré postačujú pre výkon jeho úloh

Need-to-know principle princíp ktorého uplatnovanie znamená, že subjekt má prístup, pozná alebo vlastní špecifické informácie potrebné pre výkon jeho oficiálnych povinností

Object (objekt) pasívna entita, ktorá obsahuje alebo dostáva informáciu. Z prístupu k objektu vyplýva aj prístup k informácii, ktorú objekt obsahuje.

Object reuse (opätovné použitie objektu) priradenie a opätovné použitie pamäťového média (napr. rámca stránky, sektora disku, magnetickej pásky) ktoré už obsahovalo nejaké objekty. Aby sa pamäťové médiá dali bezpečne znova použiť nesmú obsahovať zvyšky údajov predchádzajúcich objektov, ktoré boli na nich uložené.

Organizational Security Policy (Organizačná bezpečnostná politika) súbor právnych noriem, pravidiel a praktík ktoré upravujú spôsob, ako organizácia manažuje, ohraňuje a distribuje citlivú informáciu

Password (heslo) chránený/súkromný reťazec znakov, ktorý slúži na overenie identity alebo na autorizovanie prístupu k údajom

Penetration (prienik) úspešné obídenie bezpečnostných mechanizmov systému

Penetration testing (penetračné testovanie) Casť bezpečnostného testovania pri ktorom sa hodnotiaci pokúša obísť bezpečnostné mechanizmy systému. Predpokladá sa, že hodnotiaci môže používať kompletnú dokumentáciu systém, ale ináč pracuje v tých istých podmienkach ako obyčajný používateľ.

Permissions (povolenia) popis typov oprávených interacií subjektu s objektom. Príklady: čítanie, zápis, vykonávanie, pridávanie, modifikácia a odstranovanie

Personnel security (personálna bezpečnosť) procedúry prijaté na zabezpečenie toho, že personál, ktorý má prístup k citlivým informáciám má na to aj príslušné oprávnenia

Physical security (fyzická bepečnostť) použitie fyzických prekážok a kontrolných procedúr ako preventívnych opatrení a protiopatrení proti hrozbám voči zdrojom a citlivej informácii

Privacy (súkromie) (1) schopnosť jednotlivca alebo organizácie kontrolovať zberanie, uchovávanie, zdielanie a šírenie informácie o svojej osobe alebo organizácii. (2) Právo jednotlivca na ochranu informácie osobného charakteru a na definovanie oprávnených

používateľov tejto informácie a spôsobu jej použitia

Privilege (privilégium) Špeciálne oprávnenie, pridelené konkrétnemu používatelovi na vykonávanie bezpečnostne relevantných operácií

Profile (profil) podrobný bezpečnostný popis fyzickej štruktúry, komponentov, umiestnenia, vzťahov, a všeobecného operačného prostredia systému

Protection profile (PP) implementačne nezávislá špecifikácia bezpečnostných požiadaviek, ktoré má spĺňať množina možných produktov alebo systémov. Je to vysokoúrovnová abstrakcia bezpečnostného zámeru a obsahuje zdôvodnenia, funkcionálne požiadavky a požiadavky na záruky.

Recovery procedures (procedúry obnovy) činnosti potrebné na obnovu výpočtových kapacít systému a dátových súborov po zlyhaní systému

Reliability (spoľahlivosť) rozsah v ktorom sa dá očakávať že systém plní svoje funkcie s požadovanou presnosťou

Resource (zdroj) čokoľvek, čo sa používa alebo spotrebováva pri plnení funkcie

Risk (riziko) očakávaná strata následkom uskutočnenia hrozby zohľadňujúca slabé miesta systému a útočný potenciál nositeľa hrozby

Risk management (manžment rizík) celkový proces identifikácie, riadenia, eliminácie alebo minimalizácie neurčitých udalostí, ktoré môžu mať vplyv na zdroje systému. Zahŕňa analýzu rizík, analýzu cost-benefit, výber, implementáciu a testovanie, evaluáciu bezpečnosti opatrení a celkové posúdenie bezpečnosti

Role (rola) definovaný súbor funkcionálne príbuzných operácií a oprávnení potrebných na vykonávanie týchto operácií, ktoré môžu byť priradené používatelovi

Secure state (bezpečný stav) podmienka, za ktorej žiaden subjekt nemôže pristúpiť k nejakému objektu neoprávneným spôsobom

Security target (bezpečnostný zámer) produktovo špecifický popis, rozpracovávajúci všeobecnejšie požiadavky z protection profile zahrňajúci informácie/svedectvá vyrobcov o tom, ako systém/produkt spĺňa požiadavky protection profile.

Security testing (testovanie bezpečnosti) proces, ktorý sa používa na overenie toho, že bezpečnostné rysy systému sú implementované v súlade s návrhom a že sú adekvátne pre predpokladané aplikačné prostredie. Proces zahňa ručné testovanie, penetračné testovanie a verifikáciu.

Sensitive information (citlivá informácia) informácia, ktorú určila oprávnená autorita a ktorá má byť chránená pred neoprávneným zverejnením, zmenou, stratou alebo zničením, ktoré by prinajmenšom spôsobili znateľnú škodu niekomu alebo niečomu

Subject (subjekt) aktívna entita (osoba, proces alebo zariadenie) ktorá spôsobuje tok informácie medzi objektami alebo zmeny stavu systému

Threat (hrozba) činnosť alebo udalosť ktorá môže ohroziť bezpečnosť systému

Validation (ohodnocovanie) proces ohodnocovania užitočnosti systému vzhľadom a jeho účel alebo zamýšľané použitie

Verification (overovanie) proces porovnávania dvoch špecifikácií systému rozličnej úrovne za účelom zistenia, či navzájom správne korešpondujú.

Virus (vírus) samoreprodukujúci sa zlomyseľný segment programu, ktorý sa sám pripája k aplikácii, alebo inému vykonateľnému komponentu systému a nezanecháva vokajšie stopy svojej prítomnosti

Vulnerability (zraniteľné miesto) bezpečnostná slabina systému, ktoré sa dá použiť na narušenie bezpečnostnej politiky systému