Protekto de datenoj en komputilaj sistemoj

Ljubiŝa PRERADOVIĈ (BA)

Enhavo – En la verko estas prezentitaj kelkaj el la tipoj de protekto kiuj devas esti konsiderataj dum la projektado de la protekto de datenoj en komputilaj retoj. La protekto estas prezentita kiel tra uzado de mastrumsistemoj kaj kontrolo de la profiloj de uzantoj, same kiel ankaŭ tra komunikaj protokoloj, kompromita elektromagneta radiado kaj kontraŭelektrona protekto.

1. ENKONDUKO

Uzado de la komputiloj en ĉiuj homaj aktivecoj fariĝas pli kaj pli grava. Enretigo de komputiloj de la tuta planedo faros globalan vilaĝon en la informadika senco. Komputiloj transprenas ĉiujn respondecajn laborojn kaj koncentrigas en si pli kaj pli grandan kvanton da informoj. La fakto estas ke ĉi tia uzado de komputiloj portas ankaŭ multajn riskojn kaj danĝerojn: gravajn informojn povas esti perditaj kiel sekvo de neantaŭvideblaj faktoroj, vandalismo, difekto de la sistemo, aŭ misuzado de informoj.
Protekto de datenoj povas esti relative simpla, sed ankaŭ tre komplika laboro, depende de tio kiaj funkcioj kaj datenoj estas komisiitaj al la sistemo. Estas klare ke per neniaj metodoj oni povas realigi absolutan protekton, sed per konsekvenca aplikado oni povas malfaciligi faligon de la protekto.
La protekto povas esti difinita kiel grupo da metodoj, teknikoj kaj juraj normoj per kiuj oni kontrolas aliron al la datenoj flanke de programoj kaj homoj, kaj protektas fizikan integrecon de la tuta komputila sistemo, ĉu ĝi estas distriubuita ĉu ne, ĉu centralizita ĉu decentralizita.

2. MASTRUMAJ SISTEMOJ

Kadre de la protekto de mastrumaj sistemoj en la verko oni pritraktos kontrolon de enportado de virusoj (ilia neutraligo kaj prevento), rajtigo kaj identigo de la uzantoj.

2.1.1 KONTROLO DE VIRUSENPORTADO

Programoj kun virusa konduto baziĝas sur ĉefaj trajtoj de la ĝenerala arkitekturo de hodiaŭaj komputilaj sistemoj. La virusoj ekestis, antaŭ ĉio, kiel konsekvenco de la granda disvastigo de la komputiloj, respektive programistoj kaj uzantoj kies motivo prefere estas produkto ol sekureco, kaj relativa simpleco de softvaraj sistemoj kiu kaŭzas ke konstruado de virusoj estas relative facila.
Ĉar komplikeco de softvaraj sistemoj kaj hardvaraj platformoj ĉiutage kreskas, ĝi pozitive influas al malaltigo de virusaj minacoj. Ĝenerala prezo de la produkto de viruso signife kreskas. La konsekvenco estas malpli da eventualaj virusproduktantoj.
Praktikan signifon virusaj programoj kun sia malica konduto montriĝis nur ĉe la personaj komputiloj kun *MS-DOS* mastruma sistemo.
Reta kaj multprocesila ĉirkaŭaĵo favore efikas al disvastigo de viruskopioj, ĉar multaj programoj vojaĝas inter retaj nodoj kiel simplaj dosieroj, kaj ĉe la celloko efektiviĝas kaj per tio iniciatas "infekton" de aliaj programoj en la sama nodo. Efikeco de tia viruso postulas ke la komenca kaj celata nodo estu komputiloj samarkitekturaj kun la sama speco de mastruma, sistema ĉirkaŭaĵo.
Funkcioj de telekontrolo kaj teleefektiviĝo, renkontiĝantaj en protokoloj havas rektan influon al formiĝebleco de malicaj programoj.
Instalado de rezidentaj kontraŭvirusaj programoj kaj regula arĥivado de programoj (*back-up*) estas simplaj defendmeĥanismoj, se oni ne aplikas ilin tro malfrue.
Kontraŭvirusa programo devas esti simpla por adaptiĝo, uzado kaj, tre grave, por ĝisdatigo. Kontraŭvirusa softvaro, ekzemple, *Dr Solomon's Anti-Virus Toolkit* malkovris ĉiujn submetitajn virusojn kaj forigis 89% da ili, dum *Symantec* programo *Norton Anti Virus* malkovris ankaŭ ĉiujn kaj forigis 77% [6].
Krome, necesas fari rezervkopiojn, kio estas plejmalmultekoste, per instalaĵo por produktado de rezervkopioj sur bendo kiu estas almenaŭ samgranda kiel disko mem.

2.1.2 NEUTRALIGO KAJ PREVENTO

La neŭtraligo estas procedo per kiu virusa konduto estas eliminata el la ĉirkaŭaĵo. Ĉi procedo ne povas esti sekura, ĉar estas komplika kaj

postulas de la neŭtraliganto posedon de instrumentoj kaj ekspertizan nivelon almenaŭ tian kian havis virusproduktanto.
La solvo plej ofte uzata en la praktiko estas reinstaligo de mastruma ĉirkaŭaĵo.
Oni devas mencii ke sistema softvaro kaj softvara ĉirkaŭaĵo devas esti mendita rekte ĉe la produktanto, kvankam la prezo estas pli alta. Tiel oni malebligas neintencan enportadon de virusoj.
La prevento konsistas el la sistema aplikado de difinitaj teknikaj kaj ne-teknikaj agmanieroj.
a) Baza teknika agmaniero
Mediumoj portantoj de programkodo devas esti protektitaj de enskribo per mekanismo kiun ne eblas facile softvare perterpasi.
b) Baza ne-teknika agmaniero
Liveranto kaj uzanto de programa kodo devas esti reciproke ligitaj per interesoj kiuj baziĝas sur pozitivaj sociaj rilatoj.
Per apero de pli kompleksaj sistemoj, ekzemple Vindozo (*MS WINDOWS*), virusminaco perdis je intenseco. Pli kompleksaj softvaraj sistemoj ne malaltigos eblecon de apero de malicaj programoj kiel "Troja ĉevalo", krome, malicaj programoj kun eco de reproduktado ne havos tiom da programistoj kiuj povas krei ilin.

2.2 RAJTIGO DE UZANTOJ

Rajtigon de uzantoj oni enkondukas ĉe sistemoj kun pli granda sekureco. Ĝi signifas ke la uzanto efektivigas difinitan agon en la sistemo.
Ekzistas du specoj de rajtigo:
2. Rajtigo de la kerno de sistemo
3. Rajtigo de la subsistemo
Rajtigoj de la kerno de sistemo estas donitaj per procezoj. Difinita rajtigo permesas al la procezo efektivigi difinitan agon. Se rajtigo ne ekzistas, al la procezo oni ne permesas efektivigi la agon.
Rajtigoj de la subsistemo estas donitaj al uzantoj. Al uzantoj per tiu ĉi rajtigo oni ebligas uzi grupon da instrumentoj ligitaj kun iu protektita subsistemo. Ĉiu subsistemo havas propran datenbazon de uzantoj al kiuj estas permesite uzi programojn el subsistemoj.

2.3 IDENTIGO DE UZANTOJ

Identigo de uzantoj ebligas ke oni sendube konstatu identecon de la uzanto dum lia aliro al sistemo.
Ĉe iuj sistemoj oni povas enkonduki plibonigon rilate pasvorton, ekzemple:
- oni povas difini minimalan longecon de pasvorto,
- oni povas difini ĉu uzanto mem elektos pasvorton aŭ la sistemo generos grupon da pasvortoj el kiuj la uzanto elektos unu,
- eblas difini maksimuman tempodaŭron de pasvorto,
- eblas difini minimuman tempodaŭron inter du ŝanĝoj de pasvorto,
- disvolviĝis grupo da raportoj rilatantaj pasvortojn en la sistemo.

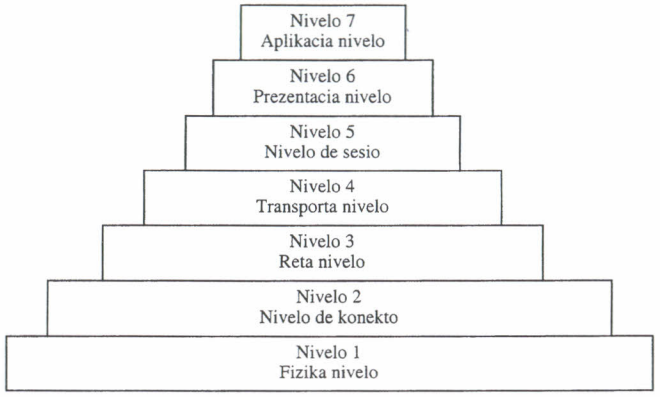
Eblas plibonigi procedurojn de aliro al la sistemo:
- eblas difini maksimuman nombron da sinsekvaj nesukcesaj aliroj de uzanto al sistemo,
- eblas difini maksimuman nombron da sinsekvaj nesukcesaj aliroj al sistemo pere de terminalo,
- eblas difini minimuman tempodaŭron inter du provoj aliri al sistemo,
- eblas difini tempon dum kiu oni devas kompletigi proceduron de aliro al sistemo,
- kiel ĉe pasvortoj ekzistas disvolvita grupo da raportoj rilatantaj aktivecojn de aliro al sistemo.

3. KOMUNIKAJ PROTOKOLOJ

Fluon de datenoj en komputilaj sistemoj oni devas protekti de subaŭskultado. La prevento estas ĉifrado de la mesaĝoj. Krom la mesaĝoj mem, estas dezirinde ĉifri ankaŭ iliajn ĉefelementojn ĉe ju pli malalta nivelo de OSI referenca modelo. Tiel de nedezirata uzanto oni kaŝas informojn pri partoprenantoj en komunikado, adresoj de sendinto kaj ricevinto, ktp.
Krome, nedezirata uzanto (atakanto) povas analizi kaj trafikfrekvencon kaj longecon de mesaĝoj por eltiri utilajn informojn el difinita kunteksto.
Por sukcesa malebligo de trafikanalizo estas necese de tempo al tempo enĵeti laŭplaĉajn hazardajn mesaĝojn en komunikan fluon kiuj estos ĉe la ricevo.

3.1 OSI MODELO DE ISO

La modelo OSI konsistas el sep niveloj aŭ tavoloj kaj preskribas kio okazas kiam du komputiloj "parolas" inter si. Ĉi modelo ebligas realigon de komunikado inter komputilaro de diversaj produktistoj.



Bildo 1. OSI modelo.

El vidpunkto de la protekto la plej grava estas nivelo de sesio aŭ nivelo de dialogoj. Ĉi nivelo ebligas ke du programoj (aŭ du partoj de la sama programo) komunikas tra reto, efektivigante sekurecan funkcion, funkcion kiu rekonas nomojn, lokigas, administras kaj faras similajn akciojn.

Sekureco de datenoj realiĝas per uzado de kriptologiaj algoritmoj kiel kun simetriaj, tiel ankaŭ kun nesimetriaj ŝlosiloj.

Simetriaj algoritmoj uzas la saman ŝlosilon por ĉifrado kaj deĉifrado, kiu estas konata nur al partoprenantoj en la komunikado.

Nesimetriaj algoritmoj uzas por ĉifrado kaj deĉifrado malsamajn ŝlosilojn; tiel ke ĉiu partoprenanto havas po unu sekretan, tielnomatan *privatan* ŝlosilon kaj la duan ŝlosilon kiu estas konata al aliaj partoprenantoj en la komunikado, tielnomatan *publikan* ŝlosilon.

Por malfaciligi kriptoanalizon en ĉifritaj komputilaj komunikadoj en la praktiko oni uzas unu plian ŝlosilon kun partatempa karaktero (simetriaj algoritmoj), aŭ paron da ŝlosiloj (asimetriaj algoritmoj).

Proponata estas la sekva metodo: Dum starigo de la logika konekto – sesio, unu el la partoprenantoj generas partatempan *ŝlosilon de sesio* kiun oni interŝanĝas en la ĉifrita formo, uzante antaŭajn ĉefajn ŝlosilojn. Post tio, ĝis la fino de la sesio, la tuta komunikado estas ĉifrata per la ŝlosilo de la sesio.

Aperas ankaŭ speco de atakoj kiuj subkomprenas duobligadon aŭ reteni mesaĝojn kaj poste reemisii ilin, en neŝanĝita formo. En tiu kazo la mesaĝoj estas vere kreitaj de rajtigitaj entitatoj en la komunikado kaj ne estas ŝanĝitaj, nur poste estas uzitaj de la atakantoj. Drasta kazo estas kiam la atakanto memorigas mesaĝojn por starigo de iu sesio, kun ĉifrita ŝlosilo de sesio, kaj poste kiam tiu ŝlosilo ne plu estas aktuala, la atakanto iamaniere ekscias ĝian valoron (ĉu per kriptoanalizo ĉu dank' al malatento de uzantoj), reemisias pakaĵojn kiuj starigas novan sesion kaj malvere prezentas sin kiel unu el la partoprenantoj de la antaŭa sesio, sen ebleco ke li estu malkaŝita. Pro tio protokoloj en siajn mesaĝojn enmetas informojn kiuj malebligas reemisiadon de la mesaĝoj.

Unu el la defendaj meĥanismoj de reemisiado de la mesaĝoj estas formigado de sekvencoj de kreskantaj numeroj kiuj estas sendataj kun la mesaĝoj. Entitatoj kiuj ricevas mesaĝojn memorigas lastajn el la vico de ĉi numeroj, tiel ke reemisiitaj mesaĝoj estas detekteblaj, ĉar entenas malnovajn valorojn, kiuj estas malpli grandaj ol tiu laste ricevita. Manko de ĉi meĥanizmo estas postulo por ĝisdatigo de lastaj numeroj por ĉiuj entitatoj.

Tial pli ofte oni uzas tempan markilon de mesaĝo kiu montras momentan daton kaj tempon de la kreado de mesaĝo, kaj entitatoj akceptas nur mesaĝojn kiuj estas tempe proksimaj al momenta reala tempo. Ĉi solvo postulas tempan sinĥronigon de komputiloj, kio ne estas facile akirebla, aparte en la kazo de geografie malproksimaj komputiloj.

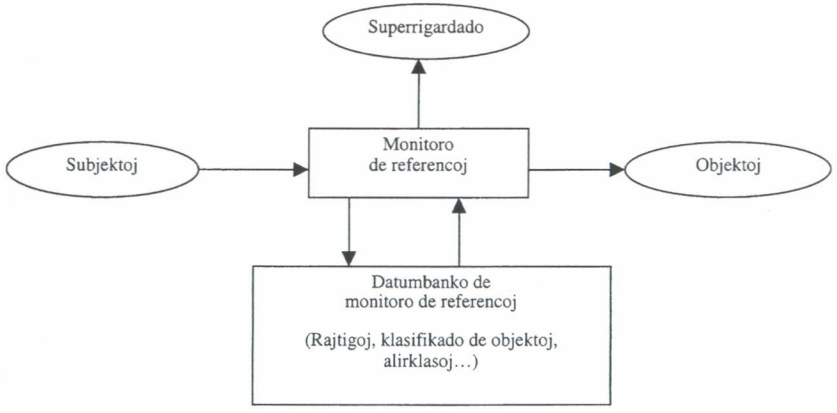
4. KONTROLO DE PROFILOJ DE UZANTOJ

Sistemo de protekto devas superrigardi kaj kontroli la agadon de ĉiu uzanto.

4.1 RAJTO DE ALIRO AL RESURSOJ

Meĥanismo de kontrolo de aliro baziĝas je koncepto "Monitoro de referencoj" kiun enkondukis *Lampson* en 1971.

"Monitoro de referencoj" estas abstrakta meĥanismo kiu troveblas kiel peranto inter aktivaj elementoj (uzantoj kaj iliaj procesoj) kaj pasivaj elementoj (dosieroj, memoraj segmentoj ktp.). Okaze de ĉiu aliro al la objektoj aktiviĝas monitoro de referencoj kiu kontrolas nivelon de rajtigo de uzantoj por koncerna operacio. Informoj pri nivelo de rajtigo estas organizitaj kiel aparta strukturo de datenoj kaj ĝi estas parto de la protekta sistemo. Por ĉiu uzanto, same kiel por ĉiu objekto kaj speco da aliro, oni povas starigi difinitan funkcion kies rezulto estas binara decido pri alirpermeso. Administradon de datenbanko en monitoro de referencoj efektivigas aparte rajtigita uzanto, tielnomata administrulo de protekto. Lia tasko estas akorde kun sekureca nivelo kiu estas aljuĝita al uzanto kaj akorde kun protektreguloj ke li aljuĝu al la uzanto difinitajn rajtojn.



Bildo 2. Koncepto "Monitoro de referencoj".

La meĥanismo de alirkontrolo ne reprezentas kompletan solvon de protekto de komputila sistemo. Ĝi estas ligita kun meĥanismoj por aŭtentigo de la uzantoj kaj kun meĥanismo por superrigardo de la sistemo.

La meĥanismo por aŭtentigo respondecas pri korekta starigo de uzanta identeco.

La meĥanismo por superrigardado havas taskon superrigardi ĉiujn agojn de uzantoj en la sistemo kaj registri tiujn aktivecojn kiuj povas endanĝerigi la sekurecon de la sistemo. Ĝi agas ankaŭ kiel malinstigilo ĉar ĝi malkuraĝigas uzantojn en iliaj provoj malobservi protektregulojn se ili scias ke ĉiuj provoj estos registritaj.

En veraj realigoj oni ne povas ĉiam fari klaran limon inter la menciitaj meĥanismoj.

4.2 MODELO DE ALIRMATRICO

Rajtigon de subjekto dum aliro al objekto ofte oni esprimas kiel listo de alirrajto. Signifo de alirrajto dependas de objekto al kiu oni aliras. Kaze de dosieroj tipa listo de alirrajtoj konsistas el operacioj *read*, *write*, *execute* kaj *own*. Se temas pri objekto de bankkonta tipo alirrajtoj povas esti prezentitaj kiel: saldo, enpago kaj elpago kaj egalas al bazaj alirtipoj faritaj sur la objekto.

La menciitaj operacioj povas esti realigitaj ĉu tra mastrumsistemo ĉu tra aplikataj programoj.

Alirmatrico prezentas konceptan modelon kiu specifas alirakton kiun ĉiu subjekto havas rilate al ĉiuj objektoj en la sistemo. Al ĉiu uzanto en la sistemo analogas unu vico en la matrico, kaj al ĉiu objekto analogas unu kolono (Bildo 3).

Kampoj en la matrico specifas alirajton por kiuj estas rajtigitaj subjektoj el la koncerna vico rilate la koncernan objekton en la koncerna kolono. Tasko de la meĥanismo por alirkontrolo estas limigi aliroperaciojn kiel estas signite en la matrico.

Evidentaj estas diversaj rajtigoj de unuopaj uzantoj rilate la objektojn.

	DOSIERO 1	DOSIERO 2	DOSIERO 3	DOSIERO 4	KONTO 1	KONTO 2
Uzanto A	Own R W		Own R W		Saldo Enpago	
Uzanto B	R	Own R W	W	R	Saldo Elpago	Saldo Enpago
Uzanto C	R W	R		Own R W		Saldo Elpago

Bildo 3. Matrico por alirkontrolo.

En la realaj sistemoj alirmatrico estus ekstreme granda, plimulto da kampoj restus neplenigitaj, ĝia traserĉado estus malfacila kaj neefika, tiel por realigo ĉefe estas uzataj du specoj da tehniko:

- listo por alirkontrolo
- listo da eblecoj

4.2.1 LISTO POR ALIRKONTROLO

Ĉimaniere formiĝas listo de ĉiuj subjektoj kun alirrajto por difinita objekto. Tiu listo aliĝas al la koncerna objekto kaj analogas al tekniko por ordigo de matrico laŭ kolonoj.
Malfaciligita estas difinado de ĉiuj rajtoj kiujn objekto havas, ĉar postulas traserĉadon de ĉiuj listoj, ligitaj kun objektoj por kiuj subjekto havas alirrajton.

4.2.2 LISTO DA EBLECOJ

Listo da eblecoj prezentas dualan aliron al listo de alirkontrolo. Al ĉiu subjekto aldoniĝas listo de ĝiaj eblecoj. La proceduro egalas al ordigo kaj konservado de matrico laŭ vicoj kio faciligas ŝanĝon de alirrajtoj por difinita uzanto. Aliflanke, malfaciligita estas difino de ĉiuj subjektoj kiuj havas aliron al difinitaj datumoj, ĉar tio postulus traserĉadon de ĉiuj listoj.

Modernaj mastrumsistemoj kutime uzas teknikon de listoj por alirkontrolo.
Kombino de ĉi du teknikoj oportunas en nuntempaj distribuitaj sistemoj. Posedo de aljuĝita listo da eblecoj eliminas bezonon por senĉesa ripetado de proceduro de aŭtentigo de uzanto en la kazoj de aliroj al diversaj serviloj.

4.3 EVIDENTIGO DE UZANTAJ AKTIVECOJ

Konfidita aplikacio aŭ protektita subsistemo difinas tipon de evento kiu enskribiĝas en spuron de eventoj.
Grupo da eventtipoj estas antaŭe difinita.
Eblas kontroli kiuj eventtipoj estos enskribitaj en la spuro de eventoj, kaj kiuj ne. Ĉi kontrolo eblas kiel en la nivelo de la tuta sistemo, same kiel en la nivelo de la uzanto.
Tipoj da eventoj kaj iliaj mallongaj priskriboj estas prezentitaj en la Tabelo 1.
En la nivelo de sistemo kontrolo realiĝas surbaze de sistema masko de eventoj, kiu entenas unu biton por ĉiu eventtipo. Ĉu la difinita tipo estos enskribita en la spuro de evento dependas de starigita koncerna bito por tiu evento.
Masko de eventoj por iu uzanto estas difinata en a nivelo de la uzanto. Por ĉiu evento en la sistemo masko de eventoj por iu uzanto enhavas unu el tri sekvontaj signoj:

- enskribi eventoj de ĉi tiu tipo,
- ne enskribi eventoj de ĉi tiu tipo,
- por ĉi tiu evento uzi signon el sistema masko de eventoj.

EVENT-TIPO	MALLONGA PRISKRIBO DE EVENTO
Startup/Shutdown	Startigo kaj Malstartigo de sistemo
Login/Logoff	Sukcesaj kaj nesukcesaj provoj de sistemaliro, malaliro de la sistemo
Process Create / Delete	Kreado kaj ĉesigo de la proceso
Make Object Available	Malfermo de dosieroj, mesaĝoj kaj semaforoj kaj aktivigo de dosiersistemo
Map Object to Subject	Efektivigo de programoj
Object Modification	Enskribado en dosieron
Make Object Unavailable	Malfermo de dosieroj, mesaĝoj kaj semaforoj kaj deaktivigo de dosiersistemo
Object Creation	Kreado de doseroj, mesaĝoj kaj semaforoj
Object Deletion	Malkreado de dosieroj, mesaĝoj kaj semaforoj
DAC Changes	Ŝanĝo de alirrajto kaj ankaŭ ŝanĝo de proprieto super dosieroj, mesaĝoj kaj semaforoj
DAC Denials	Rifuzita alirpostulo
Admin/Operator Actions	Agoj kiujn entreprenis sistemadministruloj kaj operatoroj
Insufficient Authorization	Ago ne sukcesis pro nesufiĉaj rajtigoj
Resource Denials	Nesufiĉe da memoro
IPC Functions	Sendado de signaloj kaj mesaĝoj al procezoj
Process Modifications	Ŝanĝo de efektivaj identikiloj, ŝanĝo de labordirektorio
Audit Subsystems Events	Ebligo/malpermeso/ŝanĝo de enskribado de eventoj
Database Events	Ŝanĝo en datenoj kiuj servas por kontrolo de sistema integreco
Subsystem Events	Uzado de protektitaj subsistemoj
Use of Authorization	Ago kies rajton havas nur uzanto

Tabelo 1. Eventtipoj.

Kiel unu el la protektoj oni povas enkonduki programon por identigo de terminalo, kiu kiel bazan rimedon por identigado uzas terminalan pasvorton.
Pere de ĉi tiu pasvorto komputilo rekonas terminalon de kiu difinita uzanto alkomunikas komputilon. La komputilo komparas konkretan pasvorton kun la listo de terminalaj pasvortoj kiuj "havas rajton" komuniki kun la terminalo. Se la rezulto de la komparado estas pozitiva, la konekto realiĝas.
Identigado de terminalo estas necesa por:

- malkovri provojn de nerajtigita kontakto kun la komputilo per enŝaltigo de 'nelegala' terminalo en konektlinio,
- konstato de permesitaj tempaj laborintervaloj de la konkreta terminalo,
- konstato de listo de uzantoj kiuj havas alirrajton al la konkreta terminalo,
- kontrolo de korekteco de informfluoj inter terminalo kaj komputilo,
- kontrolo de korekteco de terminala laboro.

4.4 LEGILO DE 'BAR-KODO'

Bar-kodoj, interalie, estas uzeblaj en aplikacioj kie informo pri subjekto devas esti precize enkomputiligita.
Evidentigo de laboristoj (uzantoj) estas unu el tipoj kiuj povas esti enmetitaj per bar-kodo.
Kiel ekzemplo de bar-kodo oni povas mencii *HBCS-5500* linian digitalan bar-kodon, kiu estas disponigebla por tre altaj rezolucioj kun nominala interspaco streketo/spaco de 0.13 mm (0.005 in.) ĝis 0.20 mm (0.008 in.).
Ekzemploj de legiloj de bar-kodoj estas produktoj *HEWLETT PACKARD – BAR CODE READERS 16800A kaj 16801A*.
Duobla RS-232-C (V.24) konektilo trovebla ĉe legiloj de bar-kodo 16800A kaj 16801A permesas unuopan legadon konfiguritan en vasta limo de *on-line* aplikacioj. Legilo de bar-kodoj uzeblas en rekta komunikado kun komputilo. Krom tio grupo da legiloj eblas komuniki kun komputilo tra multipleksilo. En tiu kazo dezirinda estas uzado de optikaj kabloj. Legilo de bar-kodo uzeblas inter terminalo kaj

komputilo, kaj povas esti konfigurita por transmisio ĝis komputilo, ĝis treminalo aŭ ĝis ambaŭ samtempe.

4.5 BIOMETRIA SOFTVARO

Uzanto pere de fingrospuro povas aliri al komputilaj resursoj. Ĉar la fingrospuro estas unika kaj neripetebla tio ĉi montriĝas kiel efika kaj sekureca maniero protekti aliron al sistemresursoj.

4.6 ALARMOJ

Koncepto de alarmoj antaŭvidas ke softvaro havu postulon dum funkciado atentigi pri nekutimaj okazaĵoj. La limoj de nekutimecoj estas facile difineblaj.
Nekutimeco povas esti difinita ekzemple: kiam en difinita tempintervalo sendas nekutime multe aŭ malmulte da pakaĵoj; interna temperaturo en la ejo en kiu troviĝas instalaĵo aŭ iu ajn alia parametro kiun oni deziras kontroli.

5. KOMPROMITANTA ELEKTROMAGNETA RADIADO (KEMR)

Elektromagnetaj ondoj (EMO) prezentas konstantan danĝeron por komputila ekipaĵo. Nerekta damaĝigo de komputila ekipaĵo sekve de elektromagnetaj influoj (ekzemple fulmotrafo proksime al ekipaĵo) povas damaĝi duonkonduktilajn elementojn.
EMO povas aperi rekte en la ekipaĵo, sed ankaŭ en alkondukantaj elektraj kabloj. Se la kablo por elektro aŭ transmisia kablo troviĝas en la proksimeco de tiuj alkondukantaj kabloj, stariĝas reciproka influo de tro alta tensio de unu kablo al la alia. Pro tio oni postulas ke kabloj por datentransmisio estu metataj aparte de bastensiaj kabloj. Ĉiu kablo agas kiel anteno kaj "kaptas" altajn tensiojn.
Estas necese paralele protekti ambaŭ instalaĵojn (elektro 220 V kaj linioj por datentransmisio). Samtempe gravas ke la objektoj estu protekitaj dunivele: horizontala nivelo – protektataj konduktiloj 220 V kaj vertikala nivelo - oni protektas datenligojn.
La unua paŝo en protekto estas protekto de ĉiuj komputilretaj linioj kiuj iel ajn alvenas aŭ forvenas el la domo. Tiucele oni uzas difinitajn filtrojn.

Ekstera protekto ne sufiĉas. Kablojn kiuj iras tra domo povas ankaŭ influi perturboj aperantaj en la domo, tiel oni devas protekti tutan aparataron kiu ebligas funkciadon de la reto. Ĉi protekto malebligas influon de perturboj al la komputila reto, sed ankoraŭ ne en la nivelo de ekstremaj laborstacioj. Multaj laborstacioj (ekstremaj ekipaĵoj) restas perturbeblaj, kaj oni devas protekti ankaŭ ilin.
Lastatempe aperis multaj aldonaĵoj por filtrado de perturboj kiuj disvastiĝas tra fizika portanto de komputilreto. Unu el la specoj de elektraj perturboj estas ankaŭ "intersistema bruo el alterigo". Ĝi ne ekzistas ĉe konduktilo por elektro, sed ĉe linioj por datentransmisio. Ĉi bruo ne povas esti superita per senĉesa kurentfonto, nek per linia filtro, ĉar estas ligita kun "alterigo". Tiu tensidiferenco povas atingi potenciale danĝeran nivelon. Tiam estas generata intersistema bruo, kio povas elvoki nekorektan funkciadon aŭ damaĝon de interfaco.
Protekto de ĉi tia speco de perturboj estas bone balancita kablado de ekipaĵo. Oni devas mencii ke optikaj ligoj estas imunaj ankaŭ al tiu ĉi speco da perturboj, ĉar ili estas galvane apartigitaj. Komputila ekipaĵo (ekz. monitoro) radias EMO-jn kiujn estas dezirinde bloki, kaj se tio ne eblas tiam oni devas labori el ekranigita spaco ("Faradea kaĝo'), kiu devas kontentigi specifajn karakterizajn valorojn.

6. KONTRAŬELEKTRONA PROTEKTO

Ekstera atakanto havas plej grandan eblecon de aliro al informfluo ĉe transportebla medio. Per elektromagneta senzoro oni facile subaŭskultas telefonliniojn kaj koaksialajn kablojn.
En lokalaj retoj nun estas plejofte uzataj koaksialaj kabloj. Ĝi konsistas el centra interna trakonduktanto kiu estas ĉirkaŭita per koncentra tavolo de dielektrika materialo, kiu estas superkovrita per metala mantelo. Ĉi tia kablo estas relative bone rezistema kontraŭ perturboj.
Optikaj kabloj pli kaj pli anstataŭas koaksialajn kablojn.
Por subaŭskulti informfluojn ĉe optikaj kabloj oni devas damaĝi fizikan strukturon de la optika kablo, per kio ricevata signalo estas malfortigita, kaj tiam la atako estas malkovrita.

7. KONKLUDO

En la verko oni deziris prezenti ĉiujn gravajn aspektojn de la sekureco kaj protekto en la komputilaj retoj.

Kiam difinita produkto estas aĉetata, oni kredas al produktanto ke la produkto kondutas laŭ asertoj de la produktanto. La produktuzanto ne havas eblecon kontroli tion, krom esplori la produkton dum ekspluatado. La uzanto ankaŭ neniam povas esti certa ĉu la sistemo havas aŭ ne, intence aŭ ne, transrestitan 'etan pordon' tra kiu oni povas nerajtigite eniri la sistemon.

Maniero por superi ĉi tiajn mankojn aŭ disvolvo de propraj produktoj, kio ofte estas multekoste, aŭ aldono de propraj sekurecaj kaj protektaj meĥanismoj.

En la Tabelo 2 estas prezentitaj teknikaj kondiĉoj de datenprotekto kiuj devas esti respektataj projektante informatikan sistemon. Dum projektado de informatika sistemo uzanto devas difini postulojn surbaze de kiuj oni aplikos difinitajn paŝojn kaj solvojn por protekto.

Sur la Bildo 3 oni povas vidi protektelementojn kiuj devas esti konsiderataj dum projektado, konstruado kaj ekspluatado de komputila reto.

Uzanto devas kontroli kvaliton de hardvaro kaj softvaro. Ekipaĵon estas dezirinde aĉeti de konataj kaj renomaj produktantoj, kaj softvaro, ĉiukaze, devus esti originala.

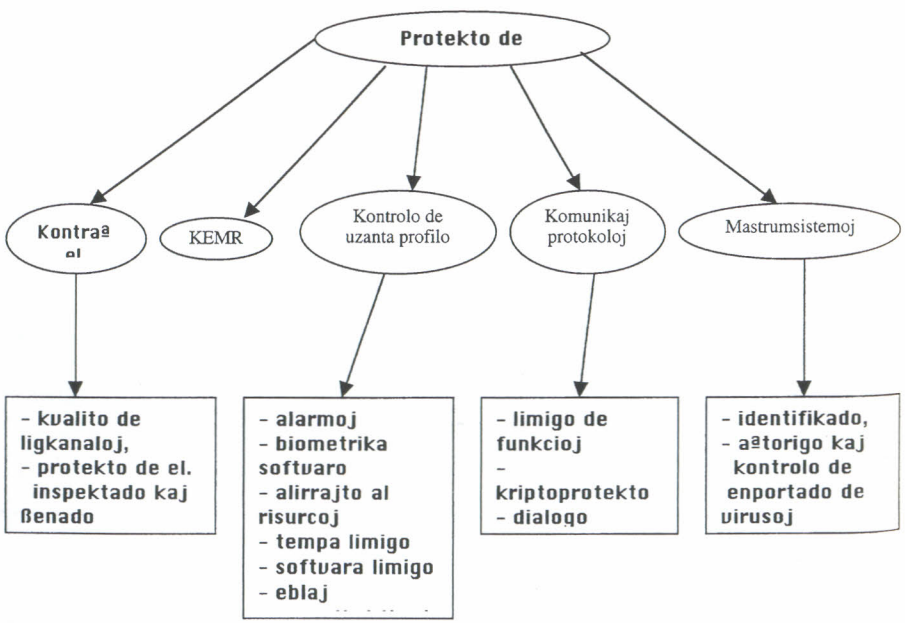
Oni devas mencii ke la homa faktoro estas ĉefa portanto de sekureco.

	Objekto de protekto	Teknikaj postuloj	Efektoj kaj kvalito
1	Datenransmisio (LAN-reto)	Kunligado de laborstacio kaj serviloj per optikaj kabloj	• neebla subaŭskultado, • eniro en LAN eblas per interrompo de kablo (kio facile diveneblas) aŭ pere de diskonduka skatolo kiu estas fizike protektata

2	Datentransmisio (WAN-retoj aŭ kunligitaj LAN-retoj)	Inter DCE (repetitoro, ponto aŭ vojplanilo) kaj DTE (modemo aŭ reta finaĵo) oni enŝaltigas en la laborstacion kriptoprotektilon aŭ modulon por kriptoprotekto	Ebligas kompletan protekton de transmisiataj datenoj
3	Protekto de datenoj (en memoro de laborstacio aŭ servilo)	Ĉifrado de datenoj per uzado de softvaraj moduloj por kriptoprotekto	Ebligas kompletan kriptoprotekton. Al datenoj povas aliri nur tiu kiu havas ĝustan internan ŝlosilon
4	Kontrolo de aliro de uzantoj	• softvaraj metodoj de raitigo de uzantoj por koncerna operacio (aliro al datenoj, prilaborado) • enportado de 'ŝlosilo' pere de bar-koda legilo de ŝildeto • enportado de ŝlosilo pere de laborstacia klavaro, • uzado de biometria softvaro • uzado de 'monitoro de referencoj'	Se ŝlosilo estas generita el sufiĉe longaj sekvencoj de hazardaj vicoj, solvo ebligas sekuran protekton
5	Protekto kontraŭ virusoj	Sisteman softvaron kaj softvaran ĉirkaŭaĵon havigi rekte de produktanto. En apliakcioj uzi meĥanismon de kontrolo de virusoj	Kvalita sistema softvaro malebligas aperon de virusoj

6	Protekto kontraŭ kompromitiga elektromagneta radiado (KEMR)	• bloki radiadon de komputilo, monitoro, printilo, servilo, • se blokado ne eblas: labori en ekranigita spaco ('Faradea kaĝo'), en retajn koduktilojn enmeti filtrojn por blokado de konduktiva KEMR	Se oni blokas EMO de instrumento aŭ oni laboras el ekranigita spaco la protekto estas kompleta kaj kvalita

Tabelo 2. Teknikaj kondiĉoj de protekto de datenoj.



Bildo 3. Elementoj de protekto.

8. LITERATURO

[1] Strucni skup: Zastita podataka u racunarskim sistemima; Zbornik radova; Beograd, 1995.

[2] Frank J. Derfler: Vodic za povezivanje; Mikriknjiga; Beograd, 1993.

[3] Dragan Markovic: Popravljanje, odrzavanje i dogradwa RS-a; SET; Beograd,1996.

[4] Grupa autora: Informatika u organima unutrasnjih poslova; Beograd, 1988.

[5] HEWLETT PACKARD: Optoelectronics Designer's Catalog, 1988/1989.

[6] Mikro 10/97; Mikroknjiga; Beograd, 1997.

Adreso de la aŭtoro:
Ljubiŝa PRERADOVIĈ, dipl. inĝ.
Altlernejo pri internaj aferoj
BA BANJA LUKA
BOSNIO-HERCEGOVINO
Respubliko Serba