ISSN 1392 - 1215 ELEKTRONIKA IR ELEKTROTECHNIKA. 2004. Nr.6 (55)

T 180 TELEKOMUNIKACIJŲ INŽINERIJA

Saugių kompiuterių sistemų kūrimo tendencijos

E. Garšva, J. Skudutis,

Radijo aparatūros katedra, Vilniaus Gedimino technikos universitetas,
Naugarduko g. 41, LT–03227 Vilnius, Lietuva, tel. +370 5 2744767, faks. +370 5 2744770, el. paštas: julius.skudutis@el.vtu.lt; eimas@aiva.lt

Įvadas

Internetui sparčiai plintant ir didėjant jo svarbai, ryškėja skaidymasis į atskirus segmentus [1] (intranetus), kurie vienas nuo kito atskiriami tarpsegmentiniais ekranais (TE). Tokie procesai, nors ir neišvengiami, prieštarauja visuotinio tinklo idėjai. Norint, kad skaidymasis į saugius, bet uždarus segmentus liautųsi, svarbu didinti visuotinio tinklo saugumą. Tinklo saugumas susideda iš kelių dalių [2]: kodavimo, saugių protokolų ir patikimos kompiuterių sistemos.

Kodavimas vaidina svarbų vaidmenį saugant informaciją nuo atskleidimo ir modifikavimo, bet pats savaime jis neapsaugo nuo vidinių grėsmių. Kodavimas yra neatsiejama autentifikavimo bei identifikavimo dalis ir turi būti integruotas į visą sistemą.

Saugūs tinklo protokolai reikalingi korektiškam tinklo funkcionavimui ir nepažeidžiamam informacijos judėjimui tarp mazgų. Šiuose protokoluose irgi dažniausiai naudojamas kodavimas.

Kompiuterių sistemos saugumo vertinimo principai, pavyzdžiui, Belo-Lapadulos [3], vertinimo kriterijai TCSE (Trusted Computer System Evaluation Criteria) [4] ir saugaus tinklo architektūros leidžia įsitikinti, ar tinklo saugumo mechanizmai yra tinkamai išdėstyti.

Aptarkime erdvę, kurioje egzistuoja sistema ir *grėsmė* jos saugumui [5] – nesvarbu, planuota ar ne, kuri gali turėti nepageidaujamą poveikį pačiai sistemai ar ten saugomai informacijai. Grėsmė gali kilti dėl kompiuterių sistemos *pažeidžiamumo*. Kuri nors prasta sistemos charakteristika sudaro sąlygas atsirasti pažeidžiamumui. Kompiuterių sistemoje sąveikauja: a) s*ubjektas* – aktyvusis elementas, galintis inicijuoti užklausą informacijai gauti ir naudoti, dažniausiai tai vartotojas, procesas arba įrenginys; b) *objektas* – pasyvusis elementas, kuris saugo arba pateikia informaciją (failai, terminalai ir t. t.).

Piktavalis veiksmas, kuriuo ieškoma sistemos pažeidžiamumo arba juo naudojamasi, vadinamas *ataka*. Taigi ataka yra grėsmės realizacija. Dažnai suplanuotų ir atsitiktinių veiksmų atskirti nepavyksta, todėl apsaugos sistema turi vienodai į juos reaguoti. Tyrėjai dažnai skiria tris pagrindines grėsmės rūšis: neteisėto informacijos atskleidimo, vientisumo pažeidimo ir atsisakymo aptarnauti.

Atskleidimo grėsmė yra informacijos patekimas ne tam asmeniui, kuriam ji skirta. Atskleidimo grėsmė kyla kiekvieną kartą, kai bandoma neteisėtai pasinaudoti kokia nors konfidencialia informacija, saugoma kompiuterių sistemoje ar perduodama iš vienos sistemos į kitą.

Vientisumo pažeidimo grėsmė yra bet koks neplanuotas duomenų, saugomų ar perduodamų, keitimas (modifikacija ar trynimas). Laikoma, kad vientisumo grėsmė dažniausiai kyla komercinėms struktūroms, o atskleidimo – valstybinėms.

Atsisakymo aptarnauti arba *atsisakymo* grėsmė kyla kiekvieną kartą, kai tam tikrais veiksmais blokuojamas priėjimas prie kokios nors kompiuterių sistemos informacijos. Realiai blokavimas gali būti pastovus, kad draudžiama informacija nebūtų pasiekiama, arba kreiptis į išteklius dirbtinai suvėlinama, todėl informacija tampa nebenaudinga. Visuotinėse kompiuterių sistemose dažniausiai pasitaiko atsisakymo aptarnauti, o vietinėse – atskleidimo ir vientisumo pažeidimo grėsmės.

Šio darbo tikslas – išanalizuoti saugumą užtikrinančių mechanizmų padėtį sistemoje, išnagrinėti siūlomas saugias tinklo architektūras ir atskleisti saugių kompiuterių sistemų kūrimo tendencijas.

Tolesnį saugumo mechanizmų ir architektūros nagrinėjimą tikslinga susieti su kompiuterių ryšio architektūra. Šiuo metu dažniausiai naudojamos dvi kompiuterių ryšio architektūros: TCP/IP protokolų rinkinio ir etaloninis OSI modelis. Plačiausiai yra paplitusi TCP/IP architektūra, o OSI modelis tapo ryšio funkcijų klasifikacijos standartu.

Saugumo mechanizmų vieta tinklo modelyje

Saugumą *fiziniame lygmenyje* [6-10] užtikrina kodavimo įtaisai, kurie statomi prieš kiekvieną mazgą. Tokia technika užtikrina duomenų srauto saugumą, kuris priklauso tik nuo abiejuose ryšio galuose esančių įtaisų ir nepriklauso nuo teikiamų paslaugų rūšies. Saugumo mechanizmų naudojimas fiziniame lygmenyje dažniausiai yra neefektyvus dėl savo statiškumo.

Saugumas *kanalo lygmenyje* turi tris jį ginančius motyvus: šis lygmuo visada egzistuoja nepriklausomai nuo naudojamų protokolų, abu tiek vartotojas, tiek paslaugos gavėjas turi galimybę apsaugoti tinklo srautą, nes bet kuris tarptinklinis įtaisas gali palaikyti saugumo mechanizmus

šiame lygmenyje. Informacijos apsaugai kanalo lygmenyje dažniausiai naudojamas kodavimas, o atpažinimas ir parašai gali būti naudojami tik mazgo ribose.

Vietiniuose tinkluose, kur dažnai prie vienos duomenų perdavimo terpės būna prijungti visi tinklo mazgai, galima perimti siunčiamą informaciją ar netgi pakeisti prieš jai pasiekiant tikslą. Protokolų rinkinyje saugumo mechanizmus galima įterpti keliose vietose: terpės pasiekimo kontrolės MAC (Media Access Control) polygmenyje arba tarp MAC ir loginio sujungimo kontrolės LLC (Logical Link Control) polygmenių. Dar galima saugumo mechanizmus koncentruoti pačiame LLC polygmenyje arba virš jo. Geresnis variantas, kurį siūlo IEEE 802.10 grupė [6], –saugaus apsikeitimo duomenimis polygmenį SDE (Secure Data Exchange) įterpti tarp LLC ir MAC. SDE užtikrina duomenų slaptumą ir vientisumą, kreipties kontrolę bei kilmės autorizaciją. SDE yra visiškai skaidrus jį supantiems polygmeniams ir nereikalauja jokių papildomų pakeitimų. Skaidrumas leidžia suderinti saugias ir nesaugias sistemas. Saugumo atributai kiekvienai asociacijai skiriami tinklu ir saugomi kaip valdymo informacijos bazės MIB (Management Information Base) saugus variantas – SMIB. Atributai, tokie kaip saugumo raktai, žymės ir identifikatoriai, reikalingi SDE polygmeniui – saugumo mechanizmams realizuoti.

Tinklo lygmenyje, kaip teigia daugelis tyrinėtojų, galima tinkamai užtikrinti informacijos saugumą, nes visi gaunami žemesnio lygmens paketai ir siunčiami aukštesnio lygmens paketai keliauja per jį. Didžiausia tinklo lygmens teigiamybė yra jo skaidrumas. Saugumas gali būti užtikrinamas be pakeitimų programose ar tinklo prietaisuose, kurie nevykdo saugumo funkcijų. IPsec yra interneto inžinerijos darbo grupės (IETF) [11] sukurtas tinklo lygmens mechanizmas, teikiantis saugaus ryšio galimybes vietiniuose ir visuotiniuose tinkluose bei internete. Jis apima: vien tik atpažinimo funkciją, vadinamą atpažinimo antrašte, kombinuotą – atpažinimo ir šifravimo funkciją, vadinamą naudingos informacijos įntegracija (Encapsulating Security Payload – ESP), ir apsikeitimo raktais funkciją. IPsec specifikacija gana sudėtinga ir apima daugybę dokumentų, iš kurių svarbiausi yra: RFC 2401, 2402, 2406 ir 2408 [12-15].

Transporto lygmenyje saugiems mazgams galima leisti bendrauti tarpusavyje nesaugioje terpėje. Šiame lygmenyje, kitaip nei tinklo, paslaugos gali pasirinkti, kurį saugumo mechanizmą naudoti, nes transporto lygmuo susijęs su teikiamų paslaugų kokybe. Trūkumas – jame sunkiau išlaikyti saugius tunelius bei konfigūruoti tarpsegmentinį ekraną. Ryšio tarp galinių mazgų saugumas gali būti realizuotas tik virš tinklo esančiuose lygmenyse, kadangi tinklo lygmenyje maršrutizavimui reikalinga informacija turi būti nekoduota. Tarp galinių mazgų realizuojamas saugumas nepasitiki tranzitiniais prietaisais, tokiais kaip maršrutizatoriai, todėl protokolais (Security Protocol) SP3, SP4 (3-ias ir 4-as saugumo protokolai), NLSP (Network Layer Security Protocol) ir TLSP (Transport Layer Security Protocol) (tinklo ir transporto lygmens saugumo protokolai atitinkamai) saugumas yra realizuojamas tarp transporto ir tinklo lygmenų [16]. Didelio pralaidumo tinkluose, kur šalia duomenų kanalo naudojamas sinchronizacijos ir tarnybinių duomenų perdavimas, toks variantas yra nelabai tinkamas, nes maršrutizacija vyksta transporto lygmenyje, o TCP yra pernelyg lėtas [7].

Virš transporto lygmens esantys sesijos, pateikimo ir taikomasis lygmenys yra realizuojami programinėmis priemonėmis ir sprendžia taikomųjų paslaugų pateikimo problemas. *Programiniuose lygmenyse* saugumo mechanizmus galima taikyti pagal naudojamų paslaugų reikalavimus. Tai pasiekiama visiems programinių lygmenų procesams ir galima pasirinktinai įtraukti į paslaugą taip didinant efektyvumą. Į programas integruotas saugumo elementas leidžia tikslingai išnaudoti programos ypatybes siekiant saugumo.

Kodavimo sistemos kanalo lygmenyje viename gale užkoduoja informaciją, o kitame atkoduoja. Aukštesniuose lygmenyse informaciją jau galima rūšiuoti: ką reikia koduoti (pvz., pranešimo duomenis), o ko ne (pvz., pranešimo antraštės). Yra mechanizmas, kuris nesunkiai nustato, kurią informacijos dalį tikslinga koduoti. Koduojant galima taikyti saugumo politikos keliamus reikalavimus, pavyzdžiui, nustatyti skirtingus saugumo lygius. Tinklo lygmenyje galima koduoti informaciją atskiruose mazguose ir taip pasiekti, kad ji nebūtų pažeista, kai keliaus per nepatikimus tinklo mazgus. Transporto ir aukštesniuose lygmenyse kodavimas turi būti neatsiejama tame lygmenyje naudojamų protokolų dalis [8].

Koks mechanizmas ir kokiame lygmenyje yra optimalus, priklauso nuo taikomos saugumo politikos konkrečiame tinklo segmente. Šiuo metu plačiausiai paplitęs sprendimas – tarpsegmentinis ekranas. Kokiu nors vienu saugumo mechanizmu ar metodu tinklo apsaugoti nepavyks, todėl naudojami keli tarpusavyje susiję mechanizmai.

Saugūs tinklo protokolai

Saugumui užtikrinti būtina tobulinti tokias interneto infrastruktūros sritis [17]: patį interneto protokolą (IP), IP maršrutizacijos protokolus, kompiuterių vardų ir jų adresų identifikavimo sistemą (DNS), tinklo valdymą, raktų, naudojamų išvardytose srityse, valdymą. Trumpai apžvelkime protokolų raidą.

IP yra interneto ašis. Abi naudojamos protokolo versijos IPv4 [18] ir IPv6 [19] neužtikrina patikimo duomenų perdavimo tarp dviejų taškų, nors į IPv6 yra įtrauktos atpažinimo ir šifravimo funkcijos. Patikimam ryšiui su vienu adresatu naudojamas TCP protokolas. Jei patikimumas nebūtinas arba jei paketai siunčiami daugeliui vartotojų, naudojamas UDP protokolas. TCP/IP modelio transporto lygmenyje yra ir interneto žinučių valdymo protokolas ICMP bei interneto narystės grupėje IGMP protokolai. ICMP protokolas labai naudingas diagnostikai, o IGMP leidžia mazgui prisijungti prie bendros gaunančių informaciją grupės arba nuo jos atsijungti.

Kanalo lygmenyje piktavalis gali: nukreipti ICMP paketus taip, kad sutriktų maršrutizacija ir atsirastų galimybė perimti kitų tinklo subjektų srautą, generuoti ICMP paketus, sukeliančius mazgo nepasiekiamumą ir atsisakymą aptarnauti. IGMP protokolo prisijungimo ar atsijungimo žinutės taip pat gali sutrikdyti aptarnavimą.

Su kylančiomis grėsmėmis kovojama naudojant kriptografinius mechanizmus: taip sumažėja grėsmė, bet didėja srautas. Galimi du kriptografiniai mechanizmai:

pridėtinis ir įterptinis. Naudojant pridėtinį mechanizmą, naudojama atpažinimo preambulė AH (Authentication Header) [13], kuri neįeina į pačios sistemos sudėtį, o antrasis mechanizmas yra paslėptas, integruotas į sistemos komponentus ESP (Encapsulated Security Payload) [14] ir glaudžiai susijęs su saugumo protokolu SP3D. ESP užtikrina informacijos slaptumą bei vientisumą ir yra nepriklausomas nuo algoritmų, t. y. senesnius kodavimo algoritmus keičiant naujesniais, mechanizmas išlieka toks pat. Šie du mechanizmai negali apsaugoti adresų skyros protokolo ARP (Address Resolution Protocol), nes jis nesinaudoja IP. Ši problema bus išspręsta perėjus prie IPv6, kur ARP pakeis adresų nustatymo protokolas, besiremiantis ICMPv6. Kadangi tarpsegmentiniai ekranai yra plačiai paplitę, manoma, kad jie turės atlikti ir srauto kodavimo bei dekodavimo funkciją, ir kodavimo raktų paskirstymo centrų funkcijas.

Internete naudojamas *dinaminis maršrutizavi-mas*, kai maršrutizatoriai patys parenka geriausią kelią konkrečiam paketui. Toks dinaminis kelio parinkimas yra būtinas besikeičiančiame pasaulyje, kuriame neišvengiama gedimų bei stichinių nelaimių [5,17]. Maršrutizatoriaus požiūriu internetas skirstomas į domenus. Domeno viduje daugiausia naudojami maršrutizacijos informacijos RIP (Routing Information Protocol), pirmiausia atveriamo trumpiausio kelio tarp domenų OSPF (Open Shortest Path First) ir tinklų sąsajos ribų BGP (Border Gateway Protocol) protokolai. Maršrutizatorių pažeidžiamumas ir maršrutų klastojimas kelia informacijos atskleidimo ir atsisakymo aptarnauti grėsmes. Numatoma, kad saugumui užtikrinti naudojamas atpažinimas ateityje stiprės. BGP protokolą pakeis tarpdomeninio maršrutizavimo protokolas IDRP (Inter Domain Routing Protocol), kuriame labiau išplėtotas kriptografinis atpažinimas. Kadangi maršrutizacijos protokolai naudojasi kitais protokolais, pavyzdžiui, BGP naudoja TCP sesiją, tai pažeidžiamumas priklauso ir nuo naudojamų protokolų saugumo. Saugiems maršrutizacijos ir kitiems mechanizmams reikalingas patogus raktų paskirstymas.

Domenų vardų sistema DNS (Domain Name System) susieja mazgų vardus su IP adresais ir kita informacija, reikalinga nutolusių sistemų darbui internete. DNS sistema yra hierarchinė ir perteklinė, t. y. vienam serveriui nustojus funkcionuoti, visai sistemai tai nepakenkia [17]. Taip istoriškai susiklostė, kad DNS neturi kriptografinio mechanizmo, todėl piktavaliai, falsifikuodami vardus, gali perimti informaciją bei efektyviai rinkti informaciją apie galimus atakų taikinius. Jau yra sukurtos technologijos (pvz., atpažinimo), kurios artimiausiu metu turėtų sumažinti DNS atakų riziką.

Tinklo valdymas daugiausia remiasi paprastuoju tinklo valdymo protokolu SNMP, kuris leidžia tiek rinkti informaciją, tiek konfigūruoti tinklo įrenginius. Šio protokolo saugumas pasiekiamas taikant koduotą atpažinimą. Kodavimas atsirado palyginti neseniai, kadangi koduojant didėja perduodamos informacijos kiekis.

Atpažinimui bei kodavimui reikalingi raktai, todėl *raktų valdymas* yra labai svarbus kriptografijos paplitimui internete. Šiuo metu paplitusios dvi technologijos: raktų paskirstymo centras, kuris naudojamas Kerberos sistemoje [20], ir Difio ir Helmano algoritmas, naudojamas generuojant dviejų informacija besikeičiančių mazgų raktus. IETF [11] plėtoja Oakley protokolą, pagal kurį viešieji raktai laikomi DNS tarnybinėje stotyje ir visi jie yra nepriklausomi nuo anksčiau sukurtų raktų. Pastaruoju metu taip pat yra kuriamas interneto saugumo asociacijų ir raktų tvarkymo protokolas ISAKMP (Internet Security Association asd Key Management Protocol) [15], kuris leis raktams turėti papildomų atributų, tokių kaip gyvavimo trukmė, saugumo lygis ir kitų.

Informacijai saugiai perduoti reikia, kad perduodančios šalys susitartų dėl saugumo užtikinimo būdo. Tokie susitarimai vadinami *saugumo sąsajomis* [9]. Šio mechanizmo reikia daugeliui saugumo protokolų, paslaugų ir mechanizmų. Raktų valdymo protokolas KMP (Key Management Protocol) palaiko simetrinį ir asimetrinį kodavimą, turi tris raktų paskirstymo mechanizmus: rankinį, centrinį ir pagrįstą sertifikatais. Jis susideda iš dalies, generuojančios raktus tarp ryšio subjektų bei tarp subjekto ir raktų centro. Sąsajos sukuriamos, prireikus atgaivinamos, o baigus ryšį ištrinamos. Saugumo asociacijų valdymo protokolas SAMP (Security Association Management Protocol) buvo sukurtas saugumui tarp įvairaus lygio tinklo įtaisų, pavyzdžiui, kompiuterio ir IP telefono, užtikrinti. Yra dviejų žingsnių procedūra: pirma sukuriamas vadinamasis saugus kontekstas, kai tarp įtaisų yra naudojamas minimalus saugumo elementų rinkinys, paskui sukuriama saugumo asociacija, įjungiant visus reikalingus saugumo elementus.

Saugumo asociacijų protokolu SAP (Security Association Protocol), sukurtu ISO, naudojasi tinklo lygmens saugumo protokolas NLSP ir transporto lygmens saugumo protokolas TLSP. Pastarasis yra daugiau teorinis taisyklių rinkinys, jo keliamus reikalavimus tenkina SAMP.

NLSP ir TLSP [10] yra patobulintos SP3 ir SP4 versijos. NLSP atlieka tas pačias funkcijas kaip ir SP3, bet papildomai užtikrina duomenų srauto konfidencialumą ir saugo kreipties režimo paslaugas paskirstydamas raktus. TLSP yra SP4, turintis kelis papildomus protokolus taikomajame lygmenyje, kurie tvarko žinučių siuntimą ir failų perdavimą.

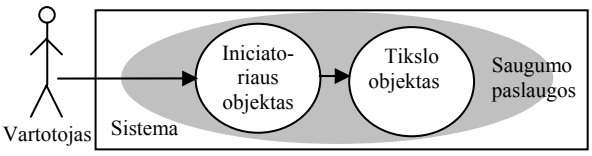
Saugaus tinklo architektūros

Saugaus tinklo architektūra buvo aprašyta dviem atviroms sistemoms skirtais standartais: **ISO 7498-2** [21] aprašo saugumo architektūrą OSI modelyje; kitas Europos kompiuterių gamintojų asociacijos **ECMA** (European Computer Manufacturers Association) standartas [22] apima platesnį atvirų sistemų spektrą. JAV nacionalinės saugumo agentūros NSA (National Security Agency) ir nacionalinis standartų ir technologijų institutas NIST (National Institute of Standards and Technology) kartu su pramonės atstovais ir mokslo įstaigomis plėtoja saugiąsias duomenų tinklų sistemas **SDNS** (Secure Data Network System) ir protokolų, kurie veikia neprieštaraudami OSI modeliui, grupę.

Pagal **ISO 7498-2** saugumo paslaugos yra realizuotos abiejų tarpusavyje bendraujančių mazgų atitinkamuose polygmeniuose. Apibrėžtos penkios pagrindinės saugumo paslaugos. *Atpažinimas* aiškiai nusako, su kuo užmegztas ryšys. Atpažinimo paslaugą

teikia N lygmens protokolas N+1 lygmens protokolui. Mazgo arba duomenų kilmės atpažinime vieno subjekto N lygmuo patvirtina N+1 lygmens tikrumą arba duomenų autentiškumą. *Pasiekimo kontrolė* kontroliuoja išteklius, kurie gali būti pasiekti per OSI sąsajas, taip pat riboja patį pasiekimą. Ji priklauso nuo atpažinimo paslaugos, kuri atpažįsta siekiantįjį išteklių. *Duomenų slaptumas* saugo duomenis nuo neautorizuoto atskleidimo. Gali būti apsaugomi visi duomenys arba pasirinkti laukai. Duomenų srauto slaptumas apsaugo informaciją nuo srauto analizės. *Duomenų vientisumas* garantuoja, kad duomenys nebus iškreipti. Įvykus pažeidimui, paslauga gali gebėti atkurti informaciją arba atpažinti pažeidimus. Gali būti taikoma visiems duomenims ar pasirinktiems laukams. *Neišsižadėjimas* reikalingas tam, kad bendraujantys mazgai neišsigintų savo siųstų ar priimtų duomenų ir neabejotų jų turiniu. Gali teikti šaltinio arba tikslo patvirtinimą. Paslaugas realizuoja aštuoni mechanizmai: šifravimas, skaitmeninis parašas, pasiekimo kontrolė, duomenų vientisumas, apsikeitimas autentifikacija, srauto užpildymas, maršrutizacijos kontrolė, notarizacija.

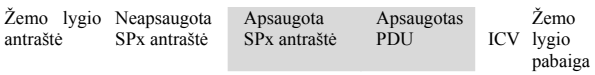
Europos kompiuterių gamintojų asociacija **ECMA** saugumo architektūros tema išdėstė atviros sistemos saugumo architektūros principus. ECMA nagrinėja tik du saugumo paslaugų tipus: atpažinimą ir kreipties kontrolę. ECMA saugumo sąveikoms taiko objektinį serverio ir kliento modelį (1 pav.). Šiame modelyje vartotojas sąveikauja su iniciatoriaus objektu (klientu), kuris dirba su tikslo objektu (serveriu). Tokiame objektiniame modelyje duomenys saugomi objekte ir abu – ir programos, ir duomenys – yra objektai. Saugumo paslaugos tarpininkauja objektams. Yra keturios saugumo paslaugų klasės: *saugaus informacijos pateikimo*, *saugumo kontrolės*, *saugumo stebėjimo* ir *kitos*. Saugumo paslaugas palaiko infrastruktūros: autentifikacijos, atributų valdymo, sąryšių valdymo, autorizavimo, audito, šifravimo.



1pav. ECMA objektinis modelis

ECMA laikosi saugaus domeno koncepcijos. Tarpdomeninė paslauga užtikrina saugų bendravimą objektams, esantiems skirtinguose domenuose. Atlikta analizė rodo, kad ECMA nagrinėja saugumą paskirstytosiose sistemose, o ISO 9478-2 – ryšių saugumą. Šių dviejų architektūrų terminologija nesuderinama, pirmoji apibrėžia penkias saugumo paslaugas ir aptaria mechanizmus, reikalingus joms realizuoti OSI modelio lygmenyse, o antrasis nusako aštuonias saugumo paslaugas ir jų realizavimą infrastruktūromis.

SDNS siūlo architektūrą, į OSI modelį integruojančią saugumo protokolus SP3 ir SP4. SDNS protokolai integruoja protokolo duomenų vienetus PDU į saugumo voką (2 pav.). Apsaugota protokolo antraštė (pateikta pradžioje) apima saugumo žymes, sekos numerius, tinklo paslaugų prieigų taškų NSAP (Network Service Access Point) adresus, sujungimų neturinčių tinklo protokolų CLNP (ConnectionLess Network Protocol) antraštes priklausomai nuo naudojamo protokolo. Vientisumo patikrinimo vertė ICV (Integrity Check Value) skaičiuojama iš apsaugotos antraštės bei PDU ir pridedama PDU pabaigoje. PDU, apsaugota antraštė ir ICV gali būti koduojami. Neapsaugota antraštė pridedama pradžioje. Ji skirta panaudotam kodavimo raktui identifikuoti.



2 pav. SDNS duomenų vienetas

Saugaus tinklo architektūros realizacijos

Yra keletas projektų, kuriuose siekiama sukurti saugias architektūras. Prie tokių priskirtina *saugios grupės (SecureGroup) ryšio sistema* [23], kuri su didele tikimybe užtikrina, kad kiekviena žinutė, kurią priėmė bet koks nepažeistas mazgas, bus priimta visų nepažeistų mazgų. Protokolas naudoja teigiamų ir neigiamų patvirtinimų bei persiuntimų sistemą, nereikalaudamas atskirų patvirtinimų iš kiekvieno žinutės gavėjo. Paskleistų (broadcast) žinučių patvirtinimai prikabinami prie pačių žinučių ir visų mazgų yra matomi. Iš patvirtinimų galima atkurti žinučių siuntimo seką, taip atpažinti bizantiškus procesus.

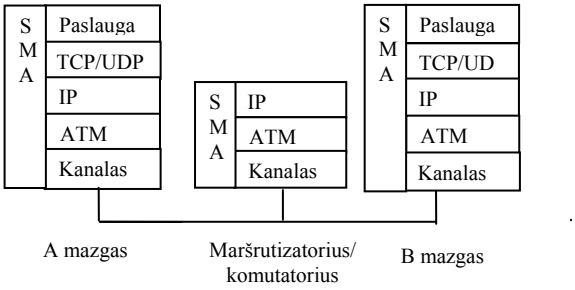
Saugus bendrasis protokolas priežastinę eilę paverčia bendrąja eile. Tada, jei atsiranda identiškų eilių, galima atpažinti klaidingą procesą ir jį nutraukti. Saugus grupės protokolas palaiko narystę grupėje, atpažįsta ir pašalina iš grupės pažeistus mazgus, nustato naujų ir atkurtų procesų tapatumą.

Dangiška (Celestial) saugumo valdymo sistema [24] kuria saugumo valdymo architektūrą, kuri gali automatiškai parinkti efektyvią saugumo politiką ir mechanizmus visame tinkle, dinamiškai konfigūruoti tuos saugumo mechanizmus visuose lygmenyse ir, pakitus sąlygoms, tuos mechanizmus perkonfigūruoti iki reikiamo lygio. Tokios sistemos pagrindiniai komponentai yra saugumo tvarkymo agentų SMA (Security Management Agent) architektūra, saugumo paslauga – programų kūrimo sąsaja API (Application Programing Interface) ir ryšio protokolas tarp SMA.

Dangiškosios sistemos architektūros pagrindą sudaro saugumo valdymo agentas SMA – programinių modulių rinkinys, išdėstytas tinklo taškuose, kuriems keliami saugumo reikalavimai (3 pav.). Tarpiniai mazgai gali neturėti SMA, bet rekomenduotina, kad kraštiniai maršrutizatoriai, kurie yra ant saugaus segmento ribos, šiuos modulius turėtų. SMA veikia už operacinės sistemos branduolio ribų, todėl pakeitimų branduolyje daryti nereikia.

SMA bendrauja su saugumo protokolais, esančiais visuose lygmenyse, ir kontroliuoja tų protokolų valdymo informaciją, todėl gali juos dinamiškai konfigūruoti. Kuriant saugų ryšį tarp dviejų mazgų, visi kelyje išsidėstę SMA turi koordinuoti savo veiksmus. Jei A mazgas nori užmegzti saugų ryšį su B mazgu, tai jis per API apie tai praneša A mazgo SMA, kartu nurodydamas, kokio saugumo lygio ir kokybės jam reikės. Tada A mazgo SMA generuoja pranešimą, kurį siunčia B mazgo SMA. Tą pranešimą perskaito visų kelyje esančių tinklo mazgų SMA

ir nurodo savo galimybes bei saugumo politikos reikalavimus, jei šie nėra įslaptinti. Tada B mazgas pagal savo galimybes bei gautą informaciją nusprendžia, kaip sukurti saugų kanalą ir kurie saugūs tarpiniai mazgai dalyvaus jį kuriant.



3 pav. Dangiška saugumo valdymo sistema

Kai kurie autoriai [26,27] mano, kad pastangos užtikrinti šiuolaikinių kompiuterių sistemų saugumą yra beviltiškos. Esą taip bandoma kovoti su pasekmėmis, o ne su jas sukėlusiomis priežastimis. Tuo tarpu pasekmės jau pasiekė tokį lygį, kad pigiau ir paprasčiau yra panaikinti priežastį. Priežastis yra pati interneto struktūra. Internetas, kaip teigia [26] autoriai, yra per daug anoniminis ir „kvailas“, jame lengva pasislėpti piktavaliui. Tačiau panaikinti anonimiškumo, kiekvienam vartotojui suteikiant eilės numerį, šiandien irgi negalima, kadangi pasaulis siekia atvirumo ir žodžio laisvės.

„Juniper Networks“ kompanija pasiūlė naujo kompiuterių tinklo infraneto projektą [27], kuris toks pat globalus kaip ir internetas, tačiau saugus, kaip banko transakcijos. Projektas numato, kad infranetą sudarys didelis kiekis mažų infranetų, sujungtų į metatinklą. Pradžioje tai bus daugiau mokamų servisų infrastruktūra, o ne informacijos perdavimo terpė.

Apibendrinimas

1. Plečiantis internetui ir didėjant jo svarbai, atsiranda segmentacija kaip būdas didinti saugumą. Saugumo užtikrinimui svarbiausi yra trys pagrindiniai dalykai: saugūs protokolai, saugaus tinklo architektūra ir duomenų kodavimas.

2. Kuriant saugaus tinklo architektūrą, daug dėmesio skiriama saugumo mechanizmų išdėstymui. Daugiausia galimybių yra saugumo mechanizmus išdėstyti programiniuose lygmenyse, bet tuo atveju jie tampa priklausomi nuo programinių lygmenų teikiamų paslaugų. Kanalo, tinklo ir transporto lygmenys saugumo mechanizmus gali naudoti nepriklausomai nuo teikiamų paslaugų. Transporto lygmenyje saugumo mechanizmai efektyviausiai apsaugo informacijos srautą per nesaugią terpę, o kanalo – apsaugo prieigą.

3. Atlikta analizė rodo, kad šiuo metu nėra universalios ir efektyvios saugumo užtikrinimo sistemos. Siūlomos saugaus tinklo architektūros yra nesuderintos: ISO 9478-2 remiasi OSI modeliu ir nagrinėja ryšių saugumą; SDNS siūlo architektūrą ir kelis protokolus, papildančius OSI protokolų rinkinį; ECMA nagrinėja saugumą paskirstytosiose sistemose.

4. Dalis autorių laikosi nuomonės, kad efektyvi grėsmių numatymo, pašalinimo ir viruso epidemijų panaikinimo sistema iš principo negali remtis šiandieniniais saugumo užtikrinimo standartais, kadangi jie, kaip ir pats internetas, atsirado be plano ir kontrolės. Todėl kuriami naujo, visiškai saugaus komunikacijų tinklo (interneto-2, infraneto ir pan.) projektai.

Literatūra

1. **John. R. Vacca.** Intranet security. Charles river media inc. Massachusetts, 1997. – 458 p.
2. **Stephen T. Walker.** Network Security: The Parts of the sum // IEEE Symposium on Security and Privacy, 1989. – P. 2-9.
3. **Bell D. E. La Padula L. J.** Secure computer systems: mathematical foundations and model. – Mitre coprp. Bedford, 1973.
4. Department of defense trusted computer system evaluation criteria. dod 5200.28-std. 1985. http://www.radium.ncsc.mil/tpep/library/rainbow/5200.28-std.html
5. **Давидович М. И., Валентинович С. Р.** Атака на Интернет. – Москва, DMK. – 1999. – 334 с.
6. IEEE Standards for Local and Metropolitan Area Networks: Standard for Interoperable LAN/MAN Security (SILS). **IEEE Std. 802.10-1998**
7. **Vijay Varadharajan.** Security in High speed Networks // Proceedings of the 21st Conference on Local Computer Networks. – 1996. – P. 2-11.
8. **William C. Birnbaum.** SP3 Peer Identification // IEEE Symposium on Security and Privacy. – 1990. – P. 41-48.
9. **W.Douglas Maughan, Amy.** Security associations: Building blocks for secure communications // IEEE Symposium on Computers and Communications. – 1995. – P. 157-163.
10. **Raju Ramaswamy.** A Security Architecture and Mechanism for Data Confidentiality in TCP/IP Protocols // IEEE Symposium on Security and Privacy. – 1990. – P. 249-259.
11. The Internet Engineering Task Force. http://www.ietf.org/overview.html
12. Security Architecture for the Internet Protocol. rfc2401. – 1998. – 66 p.
13. IP Authentication Header. rfc2402. – 1998. – 22 p.
14. IP Encapsulating Security Payload (ESP). rfc2406. – 1998. – 22 p.
15. Internet Security Association and Key Manage-ment Protocol (ISAKMP). rfc2408. – 1998. – 86 p.
16. **William E. Burr.** Security in ISDN. SP 500-189. – 1991. – 68 p.
17. **Randall J. Atkinson.** Toward a More Secure Internet// Computer. – 1997. – P. 57-61.
18. Internet Protocol. RFC 791. – 1981. – 44 p.
19. Internet Protocol, Version 6 (IPv6) Specification. RFC 2460. – 1998. – 39 p.
20. Kerberos: The Network Authentication Protocol. http://web.mit.edu/kerberos/www/
21. Informacijos apdorojimo sistemos. Atvirųjų sistemų sąryšis. Pagrindinis etalonas. 2-oji dalis. Apsaugos architektūra**.** LST ISO 7498-2:1994.
22. Security in Open Systems – A Security Framework. ECMA-TR/46. – 1998. – 86 p.
23. **Moser L. E., Melliar-Smith P. M., Narasimhan N.** The Secure Group Communication Systems // DARPA Information Survivability Conference & Exposition – Volume 2. – 2000.

24. **Chong Xu, Fengmin Gongy, S.Felix Wu,** et al. Celestial Security Management System // DARPA Information Survivability Conference & Exposition – Volume 1. – 2000.
25. Security Policy System www.ir.bbn.com/projects/pbsm/
26. **Doc Searls and David Weinberger.** World of Ends. http://www.worldofends.com/
27. J-Protect Security Solution. http://www.juniper.net

Pateikta spaudai 2004 02 26

E. Garšva, J. Skudutis. Saugių kompiuterių sistemų kūrimo tendencijos // Elektronika ir elektrotechnika. – Kaunas: Technologija, 2004. – Nr. 6(55). – P. 43-48.

Aptariamos saugių kompiuterių sistemų kūrimo tendencijos. Dėl nepakankamo saugumo kompiuterių tinklas šiuo metu skaidosi į atskirus segmentus (intranetus), kurie vienas nuo kito atskiriami tarpsegmentiniais ekranais. Tokie procesai prieštarauja visuotinio tinklo idėjai. Norint, kad skaidymasis į saugius, bet uždarus segmentus liautųsi, svarbu didinti visuotinio tinklo saugumą. Tinklo saugumas susideda iš kelių dalių: kodavimo, saugių protokolų ir patikimos kompiuterių sistemos. Dažniausiai skiriamos trys pagrindinės grėsmės rūšys: neteisėtas informacijos atskleidimas, vientisumo pažeidimas ir atsisakymas aptarnauti. Šiame darbe saugumo mechanizmai ir architektūros yra nagrinėjamos kompiuterių ryšio architektūros pagrindu ir parodoma saugumo mechanizmų vieta tinklo modelyje. Atlikta analizė parodė, kad daugiausia galimybių yra saugumo mechanizmus išdėstyti programiniuose lygmenyse, bet tuo atveju jie tampa priklausomi nuo programinių lygmenų teikiamų paslaugų. Kanalo, tinklo ir transporto lygmenys saugumo mechanizmus gali naudoti nepriklausomai nuo teikiamų paslaugų. Transporto lygmenyje saugumo mechanizmai efektyviausi yra apsaugant informacijos srautą per nesaugią terpę, o kanalo – apsaugant prieigą. Atlikta analizė rodo, kad šiuo metu siūlomos saugaus tinklo architektūros nesuderintos: ISO 9478-2 remiasi OSI modeliu ir nagrinėja ryšių saugumą; SDNS siūlo architektūrą ir kelis protokolus, papildančius TCP/IP protokolų rinkinį; ECMA nagrinėja saugumą paskirstytosiose sistemose. Šių architektūrų terminologija irgi nesuderinama. Il. 3, bibl.27 (lietuvių kalba; santraukos lietuvių, anglų ir rusų k.).

E. Garšva, J. Skudutis J. Secure Computer System Design // Electronics and Electrical Engineering. – Kaunas: Technologija, 2003. – No. 6(55). – P.43-48.

Secure computer system design trends are described in the article. Insufficient computer network security led to Internet segmentation to intranets, witch are separated by firewalls. Such processes oppose global network idea. To stop segmentation into secure, but closed segments, the global network security growth is needed. Network security consists of: coding, secure protocols and the trusted computer system. There are three kinds of threats: disclosure of secret information, consistency breach and denial of service. Security mechanisms and architectures are described showing the security mechanism position in the networking model. The analysis has shown that widest opportunities are to implement security mechanisms at application level, but then they depend on running services. Data link, network and transport levels enable security mechanism using without provided services influence. Transport layer security mechanisms are best for information transition through insecure media, while data link layer is most effective securing access. Network architectures are inconsistent: ISO 9478-2 relies on the OSI model and concentrates on interconnection security; SDNS proposes architecture and secure protocols supplementing the TCP/IP stack; ECMA analyse security in distributed systems. Terminology and structure of architectures are inconsistent. Ill.3, bibl.27 (in Lithuanian; summary in Lithuanian, English and Russian).

Э. Гаршва, Ю. Скудутис. Компьютерная безопасность и тенденции ее развития // Электроника и электротехника. – Каунас: Технология, 2004. – № 6(55) . – С. 43-48.

Обсуждаются тенденции проектирования сохранных систем. Недостаточный уровень сохранности интернета привел к его дроблению на отдельные сегменты (интранеты), которые разделены брандмауерами. Такие процессы несоответствуют идеи глобальной сети. Повышение сохранности в глобальной сети может остановить подобные процессы. Безопасность сети складывается из кодирования, сохранных протоколов и надежных компьютерных систем. Выделяются три основные типы угрозы – несанкционированное раскрытие информации, повреждение целостности и отказ в обслуживании. В данной работе механизмы и архитектуры безопасности анализируются основываясь на архитектуре связи и показывается положение механизмов безопасности в модели сети. Анализ показал, что больше всего возможностей механизмы безопасности разместить на программных уровнях, но тогда они становятся зависимыми от предоставляемых сервисов. Канальный, сетевой и транспортный уровни механизмы безопасности могут использовать независимо от предоставляемых сервисов. Механизмы безопасности на транспортном уровне являются более эффективными охраняя поток информации через небезопасную среду, а на канальном – охраняя доступ. Анализ показал, что используемые архитектуры безопасной сети несовместимы: ISO 9478-2 основывается на модели OSI и рассматривает сохранность связи; SDNS предлагает архитектуру и группу протоколов в дополнение OSI модели; ECMA анализирует безопасность распределенных систем. Терминология этих архитектур несогласованна. Ил. 3, библ. 27 (на литовском языке; рефераты на литовском, английском и русском яз.).

DOI: 10.5755/j02.eie.10868