KAUNO TECHNOLOGIJOS UNIVERSITETAS

INFORMATIKOS FAKULTETAS

KOMPIUTERIŲ KATEDRA

Vidas Žabinskas

INTERNETO SERVERIŲ APSAUGOS PRIEMONIŲ TYRIMAS

Magistro darbas

Darbo vadovas:
doc. A. Venčkauskas

KAUNAS
2004

KAUNO TECHNOLOGIJOS UNIVERSITETAS

INFORMATIKOS FAKULTETAS

KOMPIUTERIŲ KATEDRA

TVIRTINU

Katedros vedėjas

doc. dr. E. Kazanavičius

2004 05 25

INTERNETO SERVERIŲ APSAUGOS PRIEMONIŲ TYRIMAS

Informatikos mokslo magistro baigiamasis darbas

Kalbos konsultantė

Lietuvių kalbos katedros lektorė

dr. J. Mikelionienė

2004 05 25

Vadovas

doc. A. Venčkauskas

2004 05 25

Recenzentas

doc. E. Toldinas

2004 05 25

Atliko

IFM– 8/3 gr. stud.

V. Žabinskas

2004 05 25

KAUNAS
2004

T U R I N Y S

Resume

AUTHORS OF THE WORK:	V. Žabinskas
FULL TITLE OF THE WORK:	**Security tools analysis for Internet Servers**
WORK ADVISOR:	doc. A. Venčkauskas
YEAR:	2004
PLACE:	Kaunas
NUMBER OF PAGES:	57
NUMBER OF TABLES:	1
NUMBER OF PICTURES:	26

Transferring the activities to electronic space, each Internet user could be involved in a risk that the information accessed and transmitted by network might be read, retrieved and, supposedly, trespassed. Therefore, the preventive protection of personal computer and computer system security is relevant in order security gaps in a computer system would appear as less as possible.

Subject of the Work: "PC Security" Internet service website designated to check-out personal computer system security by users on their own.

Goal of the Work: computer security measures analysis and computer security control system development.

The current study contain the analysis of measures that support system to be more attack-resistant: rules necessary for network security resistance; information coding measures; actions disturbing normal system operation; actions to be undertaken in case of successful intruder attack. Requirements for the models of Internet server security and testing system were set therein. Observing the aforementioned requirements computer system security testing system was designed and implemented, system testing carried out, and system user specifications described. For flexibility purposes two check-out options were involved in the testing system: system user performs the computer IP testing himself/herself or testing is performed by a system operator with report sending.

This particular testing system should be very useful for the users because the latter would be provided by both a service (computer system testing) and a help (advices how to deal with security issues) at the same time, and as a result the users may set their labour resources on other things and save up.

1. Įvadas

1.1. Interneto serverių apsaugos priemonių aktualumas

Kai paleidžiamas Interneto serveris, jis tampa prieinamu visam pasauliui, prieinamu tampa ir patekimas į organizacijos tinklą. Dalis žmonių paprasčiausiai naudojasi pateikiama informacija serveryje, kita dalis serverio apsaugos sistemoje ieškos pažeidžiamų vietų, kad patektų prie informacijos, kuri nėra skirta viešam platinimui ar naudojimui. Bet kokiu atveju, jeigu atsiranda spragos apsaugos sistemoje, tuomet Interneto serveris gali būti panaudotas nederamai informacijai platinti, arba gali būti prarasta svarbi ir konfidenciali informacija. Kai kada įsilaužėliai gali pasinaudoti serveriu bei jo resursais, kad nesankcionuotai patektų į kitą serverį, tuo sukeldami grėsmę pirmojo serverio šeimininkui kaip įstatymo pažeidėjui. Visos šios situacijos yra gan nemalonios. Dauguma incidentų, susijusių su Interneto serveriais, įvyksta dėl neteisingos programinio aprūpinimo konfigūracijos. Programinis aprūpinimas arba priedai, kurie paleidžiami serveryje(CGI programos, SSI ir Server API priedai), gali būti grėsmės serverio saugumui priežastimi. Jeigu Interneto serverio konfigūracija suderinta, ir paleisti jame priedai pakankamai apsaugoti, tai dar nereiškia, kad serveris pakankamai saugus. Į Interneto serverį gali būti įsilaužta ir kitais būdais: per visai su juo nesusijusiu priedu arba pasinaudojus OS trūkumais ar prasta tinklo architektūra.

Apibendrinus, galima pasakyti, kad saugumo užtikrinimas gali pasirodyti kaip labai sudėtingas procesas, tačiau reikia nepamiršti, kad absoliutus aplinkos saugumas yra nerealus ir neegzistuoja jokio universalaus, susijusio su procesų saugumu, sprendimo būdo, kadangi tokie klausimai iškyla nuolat. Todėl svarbiausia užtikrinti tokį apsaugos lygį, koks yra įmanomas tuo metu.

1.2. Tiriamojo darbo tikslas

Šio tiriamojo darbo tikslas yra sukurti programinį paketą (elektroninę svetainę internete), kuriame užsiregistravę vartotojai (fiziniai ar juridiniai asmenys), galėtų patikėti savo kompiuterinės sistemos testavimą svetainės valdytojui arba atlikti testavimą patys, pasirinkę tam tikrus kriterijus.

Realaus sistemos modelio atskiroje dalyje sistemos vartotojui, pagal jo pasirinktus kriterijus, turėtų būti atliktas serverio apsaugos priemonių testavimas, ataskaitų pateikimas bei sprendimų siūlymas.

1.3. Pagrindiniai uždaviniai

- Išnagrinėti Interneto serverių apsaugos sistemų bei jų parametrų ypatumus. Taip pat būdus, kuriais gali būti sutrikdytas sistemos darbas.
- Suformuoti pagrindinius reikalavimus Interneto serverių apsaugos ir testavimo sistemos modeliui.
- Pritaikyti pasiūlyto proceso modelį konkrečiai situacijai įgyvendinti ir pateikti Interneto serverių apsaugos sistemos vartotojo sąsajos aprašymą.

2. Interneto serverių ypatumai

2.1. Informacijos elektroninėje erdvėje sauga

Žmogaus teisių visuotinėje deklaracijoje teisė į privatumą yra įvardijama kaip fundamentali žmogaus teisė. Skiriamas informacinis ir komunikacinis privatumo požymiai. Informacinis privatumas gina asmens duomenis, o komunikacinis – privačios informacijos vartojimą, perdirbimą ir saugojimą telekomunikacinėse ir informacinėse sistemose bei juos jungiančiuose tinkluose. Tai galioja visiems – tiek komerciniams, tiek valstybės paslaugų teikėjams (http://privacyinternational.org/survey).

Lietuvoje elektroninės vagystės kol kas dar nėra populiarios, bet pasauliniu mastu tai tapo jau didele problema. Visuomenės apklausos rodo, kad abejojama ar tinklalapių savininkai atvirai ir pakankamai glaudžiai bendradarbiauja su bankais, teisėsaugos organais, ar ieškoma sprendimų. Elektronine komercija besiverčiančios bendrovės linkusios slėpti informaciją apie įsilaužimus nuo savo klientų, akcininkų, partnerių ir teisėsaugos organų (http://www.gocsi.com/).

Statistikos duomenys rodo, (pagal 2002-ųjų *"Computer Security Institute" (CSI)* apklausą), kad tik 38 proc. apklaustų įmonių per pastaruosius 12 mėn. pranešė apie neautorizuoto prisijungimo arba piktnaudžiavimo atvejus; dar 21 proc. negalėjo tiksliai atsakyti, ar tokie faktai buvo. 12 proc. pranešė apie informacijos vagystės atvejus. 6% proc. pranešė apie finansinių apgavysčių atvejus (http://www.gocsi.com/).

Institucija, kuri renka, kaupia ir saugo duomenis, turi būti suinteresuota saugiu duomenų priėmimu, apsauga nuo nesankcionuoto informacijos perėmimo ryšio metu ir suformuotų duomenų bazių apsaugą nuo nesankcionuotos krypties ir duomenų sugadinimo. Interneto vartotojas, kuris gauna elektronines paslaugas, suinteresuotas, kad tinklu perduodama informacija be iškraipymų pasiektų adresatą ir ryšio metu informacija būtų nepasiekiama trečiajam asmeniui. Perkėlus savo veiklą į elektroninę erdvę, kiekvienam interneto vartotojui atsiranda pavojai, kad tinklu pasiekiama ar perduodama informacija bus nuskaityta ir, gal būt, piktybiškai panaudota. Grėsmes komunikacinių tinklų ir informacinių sistemų saugiam darbui gali sukelti bandymai prie jų nesankcionuotai prisijungti, siekiant perimti, iškreipti ar pakeisti informaciją, griaunamos virusų atakos, tyčiniai griaunamieji veiksmai, stichinės nelaimės.

McClure S., Shah S., Shah S. Hacking (2003) nurodo tris nesaugaus darbo tinkle lygmenis:

• **Tinklo lygmuo** – prie šakotuvų (angl.hub) tinkle prijungti kompiuteriai gali perimti vienas kito siunčiamus ir gaunamus duomenis; šiame lygmenyje saugumą labai padidina komutatorių (angl. switch) panaudojimas

• Duomenų bazių **serverių** lygmuo - duomenų bazių serverių apsauga.

• Informacinių **sistemų administratorių** bei kito aptarnaujančio personalo lygmuo. [1, p. 159].

Jokios apsaugos sistemos nebus efektyvios, jei aptarnaujantis personalas pedantiškai nevykdys apsaugos politikos ir nepasiduos jokioms įsilaužėlių provokacijoms. Praktika ir statistika rodo, kad įsilaužimų ir ypač atakų į kompiuterines sistemas vis daugėja. Pagal U. Black (2000) pagrindinės atakų gausėjimo priežastys:

• Interneto vartotojų skaičiaus augimas (kartu ir atakuotojų !);

• naujų prieigų prie kompiuterių atsiradimas;

• programinės įrangos, skirtos darbui tinkle, gausėjimas;

• verslo ir valdžios procesų kompiuterizacija;

• atvirojo kodo programinės įrangos populiarėjimas – atakuotojas lengviau gali surasti „skyles“ programinės įrangos išeities tekstuose [4, p. 132].

Pastarojo laikotarpio tendencija aiški: labiausiai atakuojamos yra Interneto ir duomenų bazių paslaugos, o tai reiškia, kad ypač pagausėjo įmonių, valdžios institucijų informacijos sistemų atakų. Tai kelia šių institucijų saugaus darbo riziką.

Pagrindinis betarpiškai saugumo lygį mažinantis faktorius yra prieigų prie duomenų kiekis: kuo daugiau egzistuoja prieigų prie duomenų, tuo sudėtingesnė apsauga; kuo daugiau nenumatytų, naujų prieigos prie duomenų būdų – tuo labiau neapsaugota sistema. Net vienas nenumatytas prieigos prie duomenų būdas gali reikšti visišką duomenų neapsaugojimą. Todėl ypač svarbu numatyti visus esamus ir galimus prieigos prie duomenų būdus, o ne tik priėjimą per tinklą. “Dažniausi prieigų apsaugos būdai:

• Ethernet tinklas – tinklo apsauga.

• Fizinis priėjimas – fizinė apsauga (pvz., perimetro apsauga).

• Bevielis priėjimas – bevielio tinklo apsauga + perimetro apsauga (pvz., reikia saugoti perimetrą, jei egzistuoja infraraudonųjų spindulių prieigos prie kompiuterių)” [3, p.253].

Patikimos sistemos saugumo lygis per visą jos gyvavimo laiką turi augti arba išlikti pastovus. Praėjus tam tikram laikui nuo sistemos saugumo organizavimo pabaigos, sistemos saugumo lygis taps nuliniu, kadangi per tą laiką atsiras naujų prieigos prie duomenų būdų, naujos operacinės sistemos, anksčiau nepastebėti ir niekam nežinomi operacinės ar taikomosios programinės įrangos pažeidžiamumai ir kt.

2.2. Nesankcionuotų įsibrovimų tipai

Dažniausiai net nenutuokiame, kas gali įsilaužti į mūsų kompiuterį. McClure S., Shah S., Shah S. Hacking (2003) išskiria tokius atakuotojų tipus :

- **Hakeriai – (**Lietuvių kalbos komisija siūlo vadinti **programišiais)** – jie niekada nesilaužia į sistemas tam, kad padarytų kokią nors žalą. Jie turi labai griežtus etikos įstatymus, kuriais vadovaujasi. Paprastai – tai aukštos kvalifikacijos specialistai ir samdomi firmų tam, kad patikrintų sistemos saugumą, surastų silpnas vietas ir pataisytų jas. Dažniausiai tai apsaugos programų ir ugniasienių kūrėjai, siekiantys patikrinti savo produktą;
- **krakeriai** , tarp kurių išskiriami:
- **vandalai** – dažniausiai sutinkama kompiuterinių nusikaltėlių grupė (jie dažnai kuria bei platina daug žalos pridarančius kompiuterinius virusus). Į kompiuterines sistemas jie įsilaužia tam, kad padarytų kažkokius pakeitimus, sunaikintų informacinius failus ir taip sutrikdytų sistemos vartotojus;
- **šmaikštuoliai** – tai dažniausiai paaugliai, norintys atkreipti į save dėmesį. Jiems tai tarsi iššūkis – padaryti kažką blogo ir nebūti pagautam. Tai mažiausiai pavojingi krakeriai, ir ekspertai mano, kad jų internete daugiausiai. Jie talpina į programas įvairius užrašus, paveikslėlius, garso efektus, bet specialiai sistemos negadina;
- **vagišiai** – savo veiksmais siekia materialinės ar kitokios naudos: pavogti pinigus, vykdyti pramoninį bei komercinį šnipinėjimą, vogti brangią kompiuterių programinę įrangą. Tyrimai rodo, kad dauguma krakerių – tai jauni 16-30 metų žmonės. Jie sudaro net 80 proc. visų krakerių.

Ekspertai pastebi tokias bendrąsias tendencijas: mažėja mėgėjiškų įsibrovimų procentas ir didėja įsibrovimų pasipelnymo tikslais procentas; jeigu anksčiau absoliučiai didžiausia informacijos nutekėjimo grėsmė buvo organizacijos viduje, tai šiuo metu didėja įsilaužimų iš išorės grėsmė.

2.3. Apsaugos nuo įsibrovimo būdai, taisyklės

Norint padidinti elektroninių paslaugų saugumą, reikia sukurti atitinkamą aplinką. Užsienio šalyse asmeninės informacijos, naudojamos elektroninėje erdvėje, apsaugos problemoms

skiriama gana daug dėmesio. 1996m. Japonijos elektroninio verslo asociacija parengė ir pateikė visuomenei Taisykles, kaip apsaugoti privačią informaciją, naudojamą elektroniniame versle (Guidelines for Protecting Personal Information in Cyber Business; June 1997, Cyber Business Associacion, Japan). Europos Komisija 2000 metais priėmė informacijos apsaugos vadybos standartą ISO/IEC l7799 „Information Technology – Code of practice for information security management“. Saugumo politikos kūrimas yra sudėtingas procesas, kurio svarbia sudėtine dalimi yra reglamentuojantys dokumentai. Privatumui ginti ir informacijos apsaugai užtikrinti naudojami įstatymai, savireguliacija ir technologinės priemonės. Lietuvoje privatumo teisė ir asmens duomenų apsauga yra ginama įstatymų.

Turime nemažai įstatymų – asmens duomenų teisinės apsaugos, valstybės registrų, telekomunikacijų, kurie didele dalimi suderinti su Europos Sąjungos direktyvomis ir numato pagrindinius šios srities reguliavimo principus.

Siekiant saugaus serverio eksploatavimo, siūloma laikytis tokių taisyklių (pagal http://www.citforum.ru/internet/securities/wwwsec.shtml):

1. Patalpinti Interneto serverį demitalirizuotoje (DMZ) zonoje. Sukonfigūruoti ugniasienę tokiu būdu, kad būtų blokuotos visų prievadų jungtys mūsų Interneto serveryje, išskyrus http (80 prievadas) arba https (443 prievadas).

2. Pašalinti visus nereikalingus servisus iš savo Interneto serverio, paliekant FTP (bet tik tuo atveju, jei jis iš tikrųjų reikalingas) ir saugaus prisijungimo per atstumą priemonę, pvz., SSH. Bet kuris nereikalingas, bet paliktas servisas gali tapti pašalinio žmogaus atakos pagalbininku.

3. Atjungti visas nuotolinio administravimo priemones, jei jos nešifruoja visų seanso duomenų arba vienkartinių slaptažodžių.

4. Apriboti žmonių, turinčių administratoriaus arba supervartotojo (angl. root) galimybes, skaičių.

5. Protokoluoti visus vartotojų veiksmus ir saugoti sisteminius žurnalus arba šifruota forma Interneto serveryje ar kitame savo intraneto kompiuteryje.

6. Atlikti reguliarius sisteminių žurnalų patikrinimus, kad pastebėti galimą įtartiną suaktyvėjimą. Įdiegti kelias programas-gaudykles, serverio atakų faktams aptikti (pvz., PHF-atakos išaiškinimo gaudyklę). Parašyti programas, kurios pasileidžia kiekvieną valandą ar pan., bei kurios tikrina slaptažodžių failo ir kitų kritinių failų vientisumą (būklę). Jei tokia programa aptinka pakeitimus kontroliuojamuose failuose, ji turi nusiųsti pranešimą sistemos administratoriui.

7. Pašalinti visus nereikalingus failus, tokius kaip phf, esančius direktorijoje, iš kurios gali pasileisti skriptai (pvz., iš /cgi-bin).

8. Pašalinti visas standartines direktorijas su dokumentais, kurie pristatomi su Interneto serveriais, tokiais kaip IIS ir ExAir.

9. Įdiegti visus būtinus, susijusius su sauga Interneto serverio programų pataisymus, nedelsiant, kai tik jie tapo žinomi.

10. Jeigu yra naudojamasi grafine sąsaja Interneto serverio administratoriaus konsolėje, reikia pašalinti komandas, kurios jį įjungia automatiškai, naudodamos informaciją iš .RC-pagalbinių direktorijų ir pakeisti jas rankinio jungimo komanda. Tada esant būtinybei galima naudoti grafinę sąsają, bet uždaryti ją iškart po to, kai baigiamas darbas.

11. Jei mašina administruojama per atstumą, būtina naudoti programą, užtikrinančia saugų susijungimą su Interneto serveriu (pvz., SSH). Negalima leisti susijungimų su Interneto serveriu per telnet arba neanoniminiais ftp-susijungimais (t. y. tie, kurie nereikalauja vardo ir slaptažodžio įvedimo) iš nepatikimų mašinų. Neblogai būtų taip pat suteikti tokio susijungimo galimybę tik nedaugeliui apsaugotų kompiuterių, kurie yra tam pačiame intranete.

12. Paleisti web-serverį chroot-režime (nėra žodynuose arba klaida žodyje) arba izoliuotos direktorijos režime (tokiu atveju ši direktorija yra šakninė failinės sistemos direktorija ir patekimas į failinės sistemos direktorijas negalimas), kad negalima būtų gauti priėjimo prie sisteminių failų.

13. Naudoti anoniminį FTP-serverį (žinoma, jei jis reikalingas) ir dirbti izoliuotos direktorijos režimu tai direktorijai, kuri skiriasi nuo direktorijos, įeinančios į Interneto serverio dokumentų šaknį.

14. Atlikti visus dokumentų atnaujinimus viešajame serveryje iš savojo intraneto. Saugoti Interneto puslapio originalus Interneto serveryje savo intranete, ir pirma atnaujinti vidiniame serveryje, o po to kopijuoti atnaujintus Interneto puslapius į viešąjį serverį per SSL-sujungimą. Darant tai kiekvieną valandą, išvengiama to, kad suniokotas serverio turinys bus pakankamai ilgai prieinamas internete.

15. Periodiškai skenuoti savo Interneto serverį tokiomis priemonėmis, kaip ISS arba nmap, tikrinant, ar neatsirado silpnų vietų.

16. Naudojant atakų aptikimo sistemas (angl. intrusion detection system) organizuoti susijungimų su serveriu stebėjimą. Sukonfigūruoti programą taip, kad ji skelbtų pavojaus signalą, aptikus bandymus panaudoti žinomas atakas ar įtartinus veiksmus su Interneto serveriu, bei protokoluotų tokius susijungimus detaliai analizei. Tokia informacija gali padėti pašalinti silpnąsias vietas ir sustiprinti apsaugos sistemą.

2.4. Veiksmai po įsibrovimo

CIAS rekomenduoja tokius Interneto serverio patikros žingsnius (pagal http://www.citforum.ru/internet/securities/wwwsec.shtml):

1. Atlikti visus pataisymus, susijusius su saugumu tiek dėl paties Interneto serverio, tiek dėl operacinės sistemos.
2. Pašalinti visus nereikalingus failus, tokius kaip .phf iš direktorijos su skriptais. Pašalinti standartines direktorijas su dokumentais, įdiegiamais su Interneto serveriu (pvz., IIS ir ExAir).
3. Patikrinti visus vartotojų prisijungimo vardus (angl. login) Interneto serveryje, kad įsitikinti, ar jie turi sunkiai atspėjamus slaptažodžius. Patikrinti visus servisus ir atvirus prievadus Interneto serveryje, kad įsitikinti, kad vietoj jų nebuvo įdiegti programos -„kirminai“.
4. Patikrinti, ar nėra įtartinų failų /dev, /etc ir /tmp direktorijose.

2.5. Saugumo vystymas

Administruojama saugumo politika nustato taisykles, būtinas tinklo apsaugos atsparumui.

Visų įvykių registracija. Šis punktas yra vienas svarbiausių. Į sisteminius žurnalus yra surašoma informacija apie serverio reakciją į kiekvieną užklausą. Registruotų užrašų analizė gali padėti gauti ir statistinę informaciją (pvz., kokie Interneto puslapiai populiaresni) ir informaciją, būtiną saugumui užtikrinti. Reikia įsitikinti, kad įjungta priėjimo ir klaidų registracija. Per sisteminius žurnalus galima atsekti, kas ir kur gavo leidimą prieiti. Reikia sistemingai peržiūrinėt sisteminius žurnalus ir, aptikus neįprastus užrašus, atlikti įdėmią sistemos analizę. Klaidų registracijos žurnalą reikia tikrinti ypač akylai.

Patikimos Interneto serverio kopijos saugojimas. Kopiją reikia saugoti saugiausiame kompiuteryje. Jeigu Interneto serveryje būtų pažeistas viešai prieinamos informacijos vientisumas, tai atstatymui prireiks patikimos (oficialios) kopijos. Paprastai tokia kopija saugoma kompiuteryje, kuris yra prieinamas tiktai serverio administratoriui (galbūt ir bendradarbiams, kurie atsako už talpinamą informaciją serveryje ar pan.). Pakankamai dažnai ji yra saugoma organizacijos vidiniame tinkle. Saugumui užtikrinti būtina naudoti patikimas šifravimo ir kontrolės technologijas, generuojančias kiekvieno failo kontrolines sumas. Failų kopijas ir kontrolines sumas būtina laikyti apsaugotame nuo kopijavimo arba tiktai skaitytojo teisėmis veikiančiam įrenginiui, kurį reikia laikyti fiziškai saugioje vietoje. Failų kontrolinėms sumoms generuoti galima naudoti šifravimo sistemą MD5.

Serverio administravimas per konsolę. Administravimas turi būti vykdomas per konsolę. Tokiu atveju, serveris administruojamas tiesiogiai, o ne per atstumą. Nors, kartais tai yra neįgyvendinama (pvz., organizacijose, kur serveris sunkiai prieinamas administratoriui). Jeigu yra būtinybė administruoti per atstumą, tai reikia naudoti griežtą autentifikacijos schemą prieš patenkant į Interneto serverį. Jeigu naudojamos administravimo priemonės Interneto pagrindu, tai būtina įsitikinti, kad nėra naudojama HTTP-autentifikacija Basic. Kitais žodžiais šnekant, reikia būti įsitikinusiam, kad tarp darbo stoties ir Interneto serverio slaptažodžiai nebus siunčiami nešifruota forma. Be to, reikia sukonfigūruoti Interneto serverio sistemą taip, kad būtų paliktas priėjimas iš vidinio tinklo atskiro kompiuterio.

Viešai prieinamų CGI priedų išmanymas. Naudojant šiuos priedus, reikia įsiminti, kad tas, kuris dirba su jais (išorinis konsultantas), gerai supranta kodą. Niekada neverta naudoti priedo kopijos iš nepatikimo šaltinio. Kad sužinoti apie galimas problemas, susijusias su tais priedais, kurie įdiegti Interneto serveryje, reikia dalyvauti USENET konferencijose. Pagal galimybes, priedus reikia diegti bandomajame serveryje preliminariems testavimams. Testuojant būtina pastoviai peržiūrinėti sisteminius žurnalus, kad aptikti klaidas ir perspėjimus, atsirandančius pagalbinių priedų darbo metu. Jeigu prieduose naudojamos elektroninio pašto paslaugos, tai reikia peržiūrėt ir elektroninio pašto registracijos žurnalus.

Turinio (duomenų) tikrinimas. Įsilaužėliai pakankamai dažnai keičia, modifikuoja ir pažeidžia sisteminius failus, prie kurių jiems pavyko prieiti. Kad išsaugotų nesankcionuotą priėjimą prie sistemos, jie dažnai modifikuoja sistemines programas, kurios iš pirmo žvilgsnio funkcionuoja normaliai, tačiau jose jau būna įvesti pakeitimai, leidžiantys pakartotiną patekimą į sistemą. Be to, įsilaužėliai dažnai modifikuoja ir pačius sisteminius žurnalus, kad panaikintų savo veiklos pėdsakus. Jie gali netgi sistemoje sukurti naujus failus.

Kad išvengti tokių problemų, galima lyginti failų ir katalogų atributus ir turinį su oficialia kopija. Jeigu buvo sukurtos kriptografinės kontrolinės failų sumos, tai galima lyginti esančios ir autentiškos kopijos kontrolines sumas, kad nustatyti skirtumus.

MD5 naudojimas failų turinio vientisumui patikrinti. Programa MD5 sukuria unikalią 128 - bitų failo turinio kontrolinę sumą. Patikimumas prilygsta „pirštų antspaudų" sistemos patikimumui ir ją galima naudoti tikrinant failų turinio vientisumą. Jeigu faile yra pakeistas bent vienas bitas, tai kontrolinė MD5 failo suma neatitiks pakeisto failo kontrolinės sumos, o suklastoti failą taip, kad sutaptų MD5 kontrolinė suma, yra pakankamai sunku. Svarbių sisteminių failų, priedų failų ir duomenų MD5 kontrolinių sumų rinkinys suteikia patogų būdą periodiniam tų failų vientisumui tikrinti. Jeigu buvo atlikti kai kurie pakeitimai be atitinkamų sankcijų, tai yra pagrindo teigti, kad į sistemą buvo įsilaužta, ir tokiu atveju reikia imtis

atitinkamų priemonių. Tokiu atveju, jei administratorius atliko pakeitimus, tai būtina iš naujo sukurti oficialią kopiją ir kontrolinę sumą.

2.6. Serverių apsaugos testavimo skenavimo apžvalga

Tinklas susideda iš ryšio kanalų, mazgų, serverių, darbo stočių, taikomojo ir sisteminio programinio aprūpinimo, duomenų bazių ir pan. Visi šie komponentai reikalauja, kad būtų patikrintas jų saugumo efektyvumas. Saugos analizės priemonės analizuoja tinklą ir ieško silpnųjų vietų jame, analizuoja gautus duomenis ir jų pagrindu yra sudaromos įvairaus tipo ataskaitos. Paminėsiu keletą problemų, kurias gali identifikuoti saugos analizės sistemos:

- programos „liukus" (angl. back door) ir "kirmėlės" tipo virusus;
- silpnus slaptažodžius;
- jautrumą prasiskverbimui iš neapsaugotų sistemų;
- tarptinklinių ekranų, Interneto serverių ir duomenų bazių neteisingą nustatymą.

Praktikoje egzistuoja du pagrindiniai būdai, kuriuos naudodamas skeneris tikrina pažeidžiamų vietų buvimą:

- skenavimas (angl. scan);
- zondavimas (angl. probe).

Skenavimas – pasyvios analizės mechanizmas, kurį naudodamas skeneris bando nustatyti pažeidžiamumo buvimą be faktinio jo buvimo patvirtinimo- pagal netiesioginius požymius. Šis metodas yra pakankamai greitas ir paprastai realizuojamas. Sutinkant su kompanija Cisco, šis procesas identifikuoja atvirus prievadus, rastus kiekviename tinklo įrenginyje, ir renka susijusias su prievadais antraštes, rastas skenuojant kiekvieną prievadą. Kiekviena gauta antraštė yra palyginama su taisyklių, aprašančių tinklo įrenginius, operacines sistemas ir pontencialius pažeidimus, lentele. Atlikto palyginimo pagrindu yra daroma išvada, ar yra pažeidžiamų vietų, ar ne.

Zondavimas – aktyvios analizės mechanizmas, kuris leidžia įsitikinti, ar analizuojamamas mazgas yra pažeidžiamas, ar ne. Zondavimas atliekamas imituojant ataką, kuri panaudojama pažeidžiamumui tikrinti. Šis būdas lėtesnis nei skenavimas, bet tikslesnis. Pagal Cisco, šis procesas naudoja skenavimo metu gautą informaciją detaliai kiekvieno tinkle esančio įrenginio analizei. Šis procesas naudoja žinomus atakos vykdymo metodus, kad pilnai įsitikinti numanomų

ir kitų pažeidžiamumų buvimu bei suranda tuos pažeidžiamumus, kurie neaptinkami pasyvių analizės mechanizmų, pvz., pažeidžiamumą DoS (angl. Denial of Service) tipo atakai.

Praktikoje šie mechanizmai realizuojami keliais metodais:

- antraščių tikrinimas (angl. banner check). Šis metodas atlieka eilę patikrinimų ir leidžia daryti išvadą apie pažeidžiamumus, pasikliaujant atsakymo, į skenerio užklausą, antrašte. Tai greitas ir paprastas realizuoti pažeidžiamumų aptikimo metodas. Tačiau negalima pamiršti, kad administratorius gali pakeisti užklausoms grąžinamą antraštės tekstą;
- aktyvūs zonduojantys patikrinimai (angl. Active probing check). Šis metodas taip pat skenavimo mechanizmo pavyzdys. Kita vertus, jis grindžiamas ne programinės įrangos versijos tikrinimu antraštėse, bet lygina programinės įrangos ,,skaitmeninės kopijos" fragmentus su žinomo pažeidžiamumo kopija. Analogišku pagrindu veikia ir antivirusinės sistemos. Šis metodas taip pat greitas, bet realizuojamas kiek sunkiau.
- atakų imitacija (angl. exploit check). Šis metodas priklauso zondavimo mechanizmui ir grindžiamas programinėje įrangoje esančių skirtingų defektų eksploatacija. Kai kurie pažeidžiamumai neišsiduoda, kol yra nekatalizuojami. Šis metodas, nekreipdamas dėmesio į antraštes, imituoja realias atakas. Tai patikimesnis, efektyvesnis, tačiau lėtesnis būdas. Be to, kai kuriais atvejais nerekomenduojamas šis metodas, ypač tada, kai atakos imitavimas gali sutrikdyti svarbių darbo stočių veiklą bei privesti prie nemažų laiko ir materialinių nuostolių.

Praktiškai kiekvienas skeneris atlieka saugumo analizę keliais etapais:

1.) informacijos apie tinklą surinkimas. Identifikuojami visi aktyvus įrenginiai tinkle ir nustatomi juose paleisti servisai ir demonai(paskutinis etapas negalioja naudojant saugos analizės sistemas, veikiančias OS lygyje);

2.) potencialių pažeidžiamumų aptikimas. Skeneris naudoja aukščiau aprašytą duomenų bazę ir lygina jos įrašus su surinktais duomenimis;

3.) numanomų pažeidžiamumų patvirtinimas. Skeneris naudoja specialius metodus ir imituoja tam tikras atakas, kad pasitvirtintų mazguose esančių pažeidžiamumų buvimas;

4.) ataskaitų generavimas. Surinktos informacijos pagrindu saugos analizės sistema sudaro ataskaitas, kurios aprašo aptiktus pažeidžiamumus;

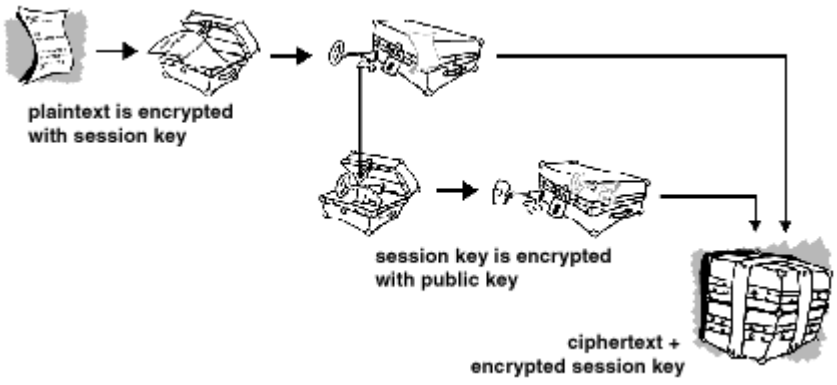
5.) automatinis pažeidžiamumų šalinimas. Šis etapas labai retai realizuojamas tinklo skeneriuose, bet dažnai naudojamas sisteminiuose skeneriuose.

2.7. Duomenų kodavimo sistemų apžvalga

“PGP *(angl. Pretty Good Privacy)* – kodavimo sistema, užtikrinanti duomenų konfidencialumą. Pradžioje ši sistema buvo naudojama tik informacijai koduoti bei elektroniniam parašui formuoti elektroninio pašto programose. Šiuo metu PGP taikoma daug plačiau: galima koduoti failus, esančius lokaliame kompiuteryje, tikrinti svarbių failų, esančių serveryje, integruotumą ir t.t. sistema naudoja RSA ir IDEA algoritmus, todėl galima pasirinkti tiek simetrinę, tiek asimetrinę kriptosistemą [2, p. 258]. Šioje sistemoje pirmą kartą buvo panaudotas „elektroninio voko“ principas.

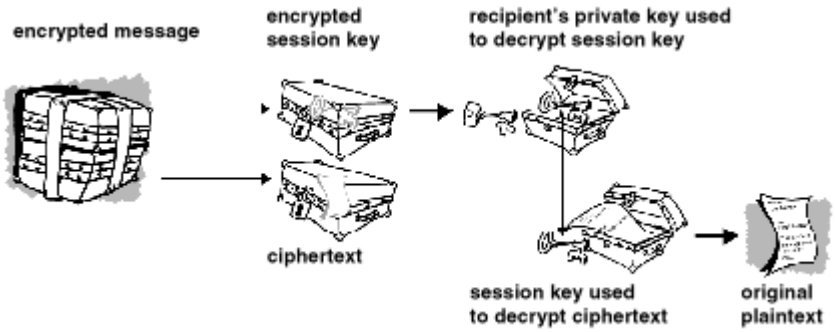
PGP yra hibridinė kriptosistema, jungianti tradicinę ir viešo rakto kriptografiją. Kai vartotojas užšifruoja atvirą tekstą su PGP, pirmiausia jis yra suspaudžiamas. Duomenų suspaudimo dėka, sutaupomas modemo siuntimo laikas, vieta diske ir svarbiausia sustiprinama kriptografijos apsauga. Yra pakankamai nemažai sukurta kriptoanalizės technikos eksploitų, kurie iš atviro teksto gali nukopijuoti šifrą. Suspaudimas sumažina tokių atvejų tikimybę. Failai, kurie yra per maži suspaudimui arba kurių negalima gerai suspausti, visai nespaudžiami.

Kaip teigia U. Black (2000), sekantis žingsnis, kuris yra atliekamas, tai sesijos rakto sukūrimas. Šis slaptas raktas yra vienkartinis. Raktas yra skaičius, atsitiktinai sugeneruotas atsižvelgiant į vartotojo pelės ir klavišų paspaudimą. Šis sesijos raktas kartu su saugiu, greitu įprastu kodavimo algoritmu koduoja atvirą tekstą ir gaunamas šifruotas tekstas. Po to, kai duomenys užkoduojami, sesijos raktas koduojamas į gavėjo viešąjį raktą ir, kartu su šifruotu tekstu, siunčiamas gavėjui.



3.2. pav. Duomenų kodavimas naudojant PGP

Dešifravimas vyksta atvirkščiai. Gavėjo PGP kopija panaudojama siuntėjo laikinam sesijos raktui iššifruoti, kurį PGP panaudoja įprastai užšifruotiems duomenims dešifruoti.

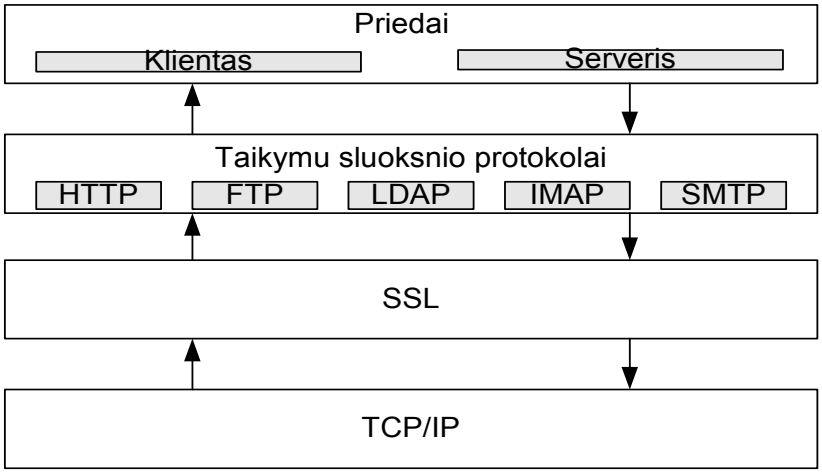


3.3. pav. Duomenų dekodavimas naudojant PGP

Dviejų kodavimo metodų kombinacija apjungia viešojo kodavimo rakto patogumą su įprasto kodavimo greičiu. Paprasto kodavimo sparta yra apie 1000 kartų didesnė, nei viešojo rakto kodavimo.

“SSL (angl. *Secure Socket Layer*) rankų paspaudimo protokolas buvo sukurtas Netscape Communications korporacijos, kad aprūpinti saugumą ir privatumą Internete. Šiuo metu jis naudojamas visuose naujesniuose Web programinės įrangos produktuose. Iki to laiko, kai kompiuteriai bus pakankamai greiti, kad aptarnautų SET, SSL sudaro pigią, ir daugelyje vietų taikomą dvipusę elektroninių atsiskaitymų sistemą” [2, p. 357].

Protokolo veikimo principas: klientas prisijungia prie serverio ir siunčia jam palaikomų kodavimo algoritmų sąrašą. Serveris atsako su algoritmo pavadinimu, savo viešu raktu, bendru raktu, bei „hash” algoritmo pavadinimu. Klientas gali patikrinti, ar viešas raktas priklauso tam serveriui. Tada klientas generuoja atsitiktinį seanso raktą ir siunčia jį serveriui, užkodavęs su serverio viešu raktu. Serveris iškoduoja seanso raktą su savo slaptu raktu ir naudoja jį duomenų kodavimui seanso metu. Klientas patikrina serverį, siųsdamas jam atsitiktinę eilutę, koduotą seanso metu. Serveris patvirtina gavimą. Daugybė algoritmų palaiko SSL protokolą, tarp kurių ir RSA, DES, IDEA ir t.t. Šis metodas naudojamas kliento-serverio autentifikavimui bei elektroninėje komercijoje.



3.4. pav. SSL sąveika su priedais

U. Black (2000) teigia, kad SSL veikia kaip tarpinis protokolas tarp TCP/IP ir taikymų sluoksnio protokolų, tokių, kaip HTTP, FTP, IMAP, ir pan. SSL naudoja TCP/IP, kaip taikymų sluoksnio protokolas, ir, jungiantis klientui, naudojančiam SSL, leidžia serveriui, naudojančiam SSL, autentifikuoti save, bei leidžia abiem kompiuteriams sudaryti šifruotą jungimąsi tarpusavyje.

"HTTPS *(angl. Secure Hypertext Transfer Protocol)* – Netscape kompanijos sukurtas produktas. HTTP yra iš prigimties nesaugus, kadangi visa informacija tarp neautentifikuotų taškų ir per visą nesaugų tinklą yra siunčiama atviru tekstu, todėl panaudojus SSL protokolą, buvo sukurtas HTTPS" [2, p. 369].

Jis leidžia klientams ir serveriams autentifikuotis sertifikatų pagalba, kurie turi būti suteikti sertifikatų agentūroje. Kliento Interneto naršyklė turi palaikyti SSL, ką dauguma naršyklių ir daro (Mozilla, MSIE, Konqueror, Opera, Lynx, w3m). HTTPS naudoja ne 80 prievadą kaip HTTP, o 443. SSL naudoja 40-bitų raktą RC4 kodavimo algoritme, kuris vertinamas kaip pakankamas kodavimo laipsnis komerciniams tikslams. Prieš klientui ir serveriui užmezgant ryšį, jie tikrina ir derina SSL protokolo versijas ir sukuria unikalų sesijos ID. Jeigu serverio sertifikatas yra nežinomas klientui, klientas pasirenka, ar jam priimti ar atmesti sertifikatą. Serveris taip pat gali reikalauti sertifikato iš kliento. Tuomet serveris ir klientas pasidalina bendrą raktą, kuris leidžia koduoti ir dekoduoti vienas kitam siunčiamus pranešimus.

2.8. Projekto analogai ir jų palyginimai

Projektą būtų įmanoma įgyvendinti ir kitais būdais, nei integruoti į interneto serverį (pvz, sukurti kaip nepriklausomą programą ir ją pardavinėti įrašytą į kompaktinius diskus), bet ji būtų ne tokia efektyvi kainos požiūriu, o taip pat būtų sunkiau atnaujinti informaciją, kuri labai greitai sensta. Kompaktinių diskų platinimo procedūros taip pat užimtų pakankamai daug brangaus laiko ir kitų sąnaudų.

Atliekant panašių sistemų paiešką ir analizę galima pastebėti, kad lietuviškų svetainių internete, kurios teiktų tokias paslaugas kaip "PC Security" nėra. Tokios paslaugos Lietuvoje dar tik žengia pirmuosius žingsnius. Tuo metu užsienyje tiek firmų, tiek personalinių kompiuterių savininkai supranta, kokios gali būti pasekmės, jei jų svarbi informacija pateks į netinkamas rankas.

Kompiuterinių sistemų saugumo patikrinimo portalai ar svetainės, kurias čia apžvelgsiu, yra registruotos užsienyje ir veikia jau kurį laiką. Šias paslaugas teikia tokios firmos

kaip “Security Metrics” (http://www.securitymetrics.com), “AuditMyPc” (http://www.auditmypc.com), “Shields UP!!” (http://grc.com) ir kt.

Savo darbe aš apžvelgsiu šias saugos tikrinimo sistemas.

“Security Metrics” savo esamus ir potencialius klientus pasitinka patraukliu akiai dizainu (3.3. pav.).

pav. 3.3. “Security Metrics” portalas

Šio portalo teikiamos paslaugos:

- *preivadų skenavimas.* Praskenuojamos kompiuterių sistemos, pateikiamos ataskaitos realiu laiku;
- *atskirų kompiuterių tikrinimas.* Ši paslauga atlieka kompiuterinės sistemos saugos patikrinimą. Esant tam tikriems pažeidimams, teikiama pagalba ištaisymo klausimais;
- *konsultacijos.* Teikiamų konsultacijų spektras labai platus, pradedant konsultacijomis telefonu iki korporacijos tinklų audito;
- *internetinės svetainės ar portalo sertifikavimą.* Užsiregistravus “Security Metrics” sistema tikrina registruotas svetaines pagal tam tikrus saugumo kriterijus. Toms svetainėms, kurios atitinka tam tikrus saugumo reikalavimus, yra suteikiamas “Security Metrics” sertifikatas;
- *perimetro tikrinimas.* Atliekama nuodugni pažeidžiamumo atestacija tinkle esantiems kompiuteriams. Yra galimybė klasifikuoti kompiuterius pagal rizikos grupes. Automatinė tinklo atpažinimo funkcija leidžia automatiškai skenuoti

visus tinklo kompiuterius nurodytu laiku. Kai kompiuterio sistemos saugos rizika padidėja, klientas gauna įspėjimą paštu.

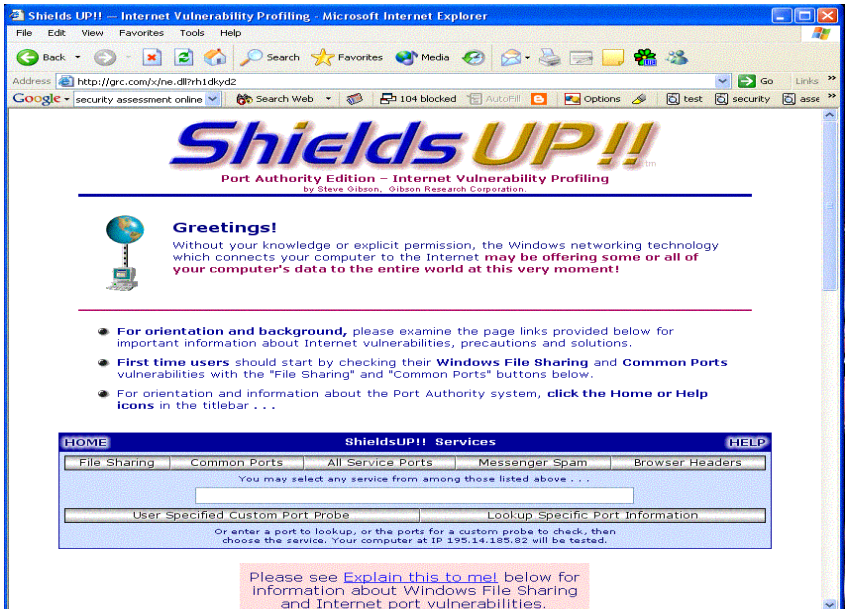
“AuditmyPC” yra kitas tokio tipo pavyzdys (žr. 3.4. pav.).

pav. 3.4. “AuditmyPC” portalas

Saugumo sistemos patikrinimas susideda iš trijų pagrindinių etapų:

- ugniasienės testas. Jis skirtas nustatyti tuos prievadus, kurių yra klausomasi. Tai labai svarbu ir gali iškelti į paviršių tūnantį virusą, kuris gali būti užsimaskavęs kaip draugiška aplikacija. Tai gali suteikti piktavaliui visišką sistemos ir saugos kontrolę. Šis testą galima atlikti pasirinkus kelis būdus:
  - ✓ kompiuterinės saugos naujokams skirtas testas. Šis testas patikrina tuos prievadus, kuriuos dažniausiai naudoja sistema, bei virusus ir “kirmeles”;
  - ✓ sudėtingesnis ugniasienės testas. Galima skenuoti standartinius prievadus nuo 1 iki 65535, arba tik tuos, kurie yra įrašomi. Šis ugniasienės testas yra padalytas į tam tikrus blokus. Tai apsaugo nuo atsitiktinių DOS atakų ugniasienės tikrinimo metu;
- „pop up” blokuotojo testas. Jis patikrina ar turimos priemonės yra veiksmingos prieš nuolat išlendančius langus;
- įvairių šnipinėjimo programų testas. Jis patikrina ar kompiuteris neturi populiarių šnipinėjimo agentų ir silpnųjų, pažeidžiamų naršyklės vietų. Šio testo tikslas yra pademonstruoti, kad neteisinga naršyklės konfigūracija ir nereguliarus pataisymų diegimas ugniasienę gali paversti beverte.

“Shields UP!!” (http://grc.com) dar viena tokio tipo sistema, kuri teikia panašias paslaugas, kaip ir prieš tai vardintos sistemos, tačiau siūlo kitokį paslaugų paketą.



pav. 3.5. “Shields UP!!” portalas

Šios sistemos meniu galima pasirinkti tokius testavimus, kaip:

- failų dalijimosi (angl. *File sharing*) testas. Naudojant tiek TCP tiek UDP protokolus yra vertinama slaptažodžių apsauga. Taip pat sistema testuojama ir failų dalijimosi pažeidžiamumams aptikti;
- dažniausiai naudojamų prievadų skenavimas. Čia autorius surinkęs 26 prievadus, kuriais, jo nuomone, gali būti pasinaudota, norint patekti į svetimą sistemą;
- visų prievadų skenavimas. Šioje dalyje yra skenuojami 1056 prievadai (0-1055). Rezultate papildomai įtraukiama informacija apie tuos prievadus, kuriuos gali blokuoti kliento Interneto paslaugų tiekėjas, patikrinama NAT maršrutizatoriaus WAN-dalies apsauga. Ataskaitoje yra pateikiama išvada, ar kliento testuojama kompiuterinė sistema atitinka “TruStealth” analizės kriterijus ar ne;
- naršyklės antraštės analizė. Pateikiama informacija apie apie kliento/serverio architektūros seanso metu vykstantį informacijos keitimąsi tarp kliento ir serverio. Suteikiama galimybė realiu laiku analizuoti kliento naršyklės Internetu siunčiamą informaciją serveriui, jei naudojamas “GET” metodas.

Šiame portale, be kita ko, gausu informacijos bei nuorodų kompiuterinės saugos klausimais.

Taigi, kaip matome iš aprašymo tiek SecurityMETRICS teikiamos paslaugos, tiek AuditMyPc bei Shields UP!! teikiamos paslaugos yra tos pačios paskirties, visos jos skirtos užtikrinti kompiuterio saugumą, skiriasi tik užtikrinimo būdai.

Lentelė 3.1. Kriterijų palyginimas

Kriterijai	Shields UP!!	AuditMyPc	Security Metrics
Nemokamos paslaugos			
Paprastasis prievadų skenavimas	Taip	Taip	Taip
Skenuojamų prievadų skaičius	26	N	22
Sudėtingesnis prievadų skenavimas	Taip	Taip	Ne
Pasirinktų prievadų skenavimas	Taip	Taip	Ne
Pažeidžiamų vietų skenavimas	Taip, dalinai	Taip, dalinai	Ne
Pop-up langų blokuotojo testavimas	Ne	Taip	Ne
Mokamos paslaugos			
Sudėtingesnis prievadų skenavimas	Ne	Ne	Taip
Perimetro skenavimas	Ne	Ne	Taip
Pažeidžiamų vietų skenavimas	Ne	Ne	Taip
Svetainių, portalų sertifikavimas	Ne	Ne	Taip
Kitos paslaugos			
HTTPS protokolo naudojimas	Taip	Ne	Taip
Įvairios informacijos ir nuorodų talpinimas, padedantis spręsti saugos problemas	Taip	Taip	Taip
Galimybė klientui patikėti savo IP adresų skenavimą saugos portalo sistemos valdytojui	Ne	Ne	Taip*

*- tais atvejais, kuomet klientas užsisako perimetro arba svetainės(portalo) sertifikavimo paslaugą

N- nėra duomenų

Atlikus panašių sistemų palyginimą galima padaryti tokias išvadas:

“Security Metrics” daugiau skirta didelėms kompanijoms, kurios turi vidinį tinklą, nors tiekia paslaugas ir pavieniams vartotojams. Tai rodo tokių paslaugų teikimas, kaip perimetro tikrinimas bei galimybė gauti internetinio puslapio saugumo sertifikatą. Mano manymu, paprastam vartotojui šios paslaugos nėra aktualu.

“AuditMyPc” ir “Shields UP!!” teikiamos paslaugos yra orientuotos daugiau į pavienį vartotoją. “Shields UP!!” privalumas yra tai, kad jų svetainėje http://grc.com/PortDataHelp.htm

galima rasti detalų prievadų aprašymą. Šis puslapis yra skirtas ne tik kompiuterių specialistams, ar žmonėms, kurie jau ne pirmą kartą susiduria su kompiuterio saugumo problemomis, bet ir paprastam vartotojui, kuris nori apsaugoti kompiuteryje esančius duomenis. Tuo tarpu “Security Metrics” labiau skirtas jau profesionalesnei kompiuterių apsaugai ir paprastas vartotojas turi turėti pakankamai žinių norėdamas pasinaudoti jų paslaugomis.

3. Reikalavimų specifikacija

3.1. Projekto užsakovai

“PC Security” projekto užsakovas yra UAB” Kompiuterinė sauga”.

3.2. Projekto vykdytojai

“PC Security” projekto vykdytojas ir darbą vykdantis asmuo yra Kauno Technologijos Universiteto Informatikos fakulteto Informacinių Technologijų (IFM-8/3) magistrantas V. Žabinskas

3.3. Projekto realizavimo terminai

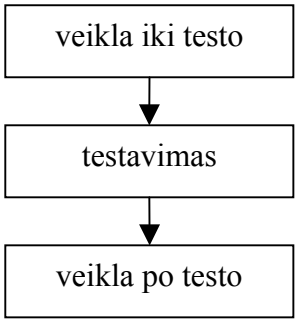
“PC Security” projekto realizacija – programinio produkto, atitinkančio reikalavimus, pristatymas numatomas 2004 metų gegužės-birželio mėn.

3.4. Programinio produkto vartotojai

Programinio produkto (“PC Security” pavadinimu) vartotojais gali būti visi fiziniai ir juridiniai asmenys, kuriuos domina jų serverių saugumas interneto platybėse ir jie perka tokias elektronines paslaugas, kaip serverio apsaugos sistemų testavimą realiu laiku ar patvirtinus sistemos administratoriui.

Interneto naršytojai, turintys interneto naršyklę ir norintys naudotis šia sistema, turėtų jungtis prie sistemos tam tikru interneto adresu (http://www.meet.serveriai.lt/security/). Ši sistema padės vartotojui įvertinti serverio apsaugos sistemų padėti ir apsispręsti skirti daugiau dėmesio ir priemonių tam, kad duomenys testuojamajame serveryje būtų saugiau pasiekiami tik registruotiems vartotojams.

Tuo pačiu siekiama vartotoją kuo labiau supažindinti su galimais esamų problemų sprendimo variantais,- teisingai nukreipti papildomų išlaidų skyrimu, programinių paslaugų ar serverio aptarnavimo specialistų paslaugų pirkimu. Patį procesą galima skaidyti pakopomis, pradedant veikla iki apsaugos sistemos testavimo ir baigiant veikla (aptarnavimu, priežiūra) po sistemos testavimo (3.1. pav.).



pav. 3.1. *Vartotojo veiklos pakopos įsigyjant sistemos testavimo paslaugą*

Paslaugų pirkimas (užsakymas) įvyksta po to, kai vartotojas suvokia problemos egzistavimą ir racionaliai ją išsprendžia. Vartotojai atlieka daug veiksmų, tokių kaip informacijos ieškojimo, alternatyvų įvertinimo, užsakymo etapus. Siūlomos esamos problemos sprendimo alternatyvos – tęsti naudotis tuo pačiu programiniu paketu (įdiegus pataisas), arba pasiūlyti tai dienai jau pagerintus analogiškus produktus.

Taip apsaugos sistemų gamintojai gali sekti pagamintų sistemų galimybes būseną ir esant poreikiui rūpintis paslaugos ar prekės popardaviminiu aptarnavimu vartotojui, analizuoti gaunamą informaciją ir tobulinti gaminius. Dar geriau, kai pats vartotojas parašo problemas su kuriomis susidūrė eksploatuojant serverį, apsaugos sistemą, ir svetainėje realiu laiku ar sudėtingesniu atveju po kiek laiko gauna informaciją, kaip išspręsti problemą ar pagerinti esamą situaciją.

Tai patariamojo tipo informacija. Ji nėra pirmo svarbumo, ir tuo pažymima, kaip teisingai reikėtų naudoti-vartoti paslaugas bei įrangą, kad ji veiktų pagal savo galimybes ir tausotų save, atitinkamai pagal apkraunamumo-panaudojamumo lygį.

Duomenų surinkimo, analizės ir pateikiamų ataskaitų bei patarimų sistemai, gamintojų ir vartotojų ryšiui suartinti, visi prietaisai galėtų turėtų būti jungiami į bendrą tinklą. Kadangi duomenų bazės ir sisteminamos informacijos srautai būtų labai dideli, tai tokiose aptarnavimo vietose reikalingas spartus ryšys ir galimybės patikimai saugoti ypatingai dideles duomenų bazes.

Šiose duomenų bazėse būtų kaupiama informacija ne tik apie paslaugų vartotojus, bet ir jų gamintojus – diegėjus, kurie vėliau pateiktų galimus iškilusių sudėtingesnių klausimų sprendimo variantus.

Ir taip su kiekviena naujai įsigyta (ar norint įsigyti) paslauga,- vyksta kliento aptarnavimo procesas nuo paslaugos įsigijimo iki jos atsisakymo, stebint esamą būklę, analizuojant ir siūlant alternatyvas, naujus gaminius, žinant vartotojo poreikius, pasirinkimo aktualumą.

3.5. Programinio produkto tikslas

Programinio produkto tikslas – sukurti svetainę internete, kuriame užsiregistravę vartotojai, galėtų “PC Security” ar kitai nepriklausomai firmai patikėti galėtų patikėti savo kompiuterinės sistemos testavimą svetainės valdytojui arba atlikti testavimą patys

Kaip jau buvo minėta, Lietuvoje apie šią problemą dar nėra plačiai kalbama, todėl, kad Lietuvoje Internetu kol kas naudojasi palyginti mažai žmonių. Didžiosiose kompanijose kompiuteriuose esančių duomenų saugumu rūpinasi kompiuterių specialistai. Kadangi jos turi pakankamai dideles pajamas, gali samdyti žmogų, kuris prižiūrėtų, kad nebūtų iš duomenų bazių vagiama informacija. Tuo metu mažosios firmos, kuriose dirba nedaug darbuotojų ir kurių pajamos nėra pakankamos, kad galėtų samdyti kompiuterių specialistą yra neapsaugotos, iš jų gali būti pavogta svarbi informacija.

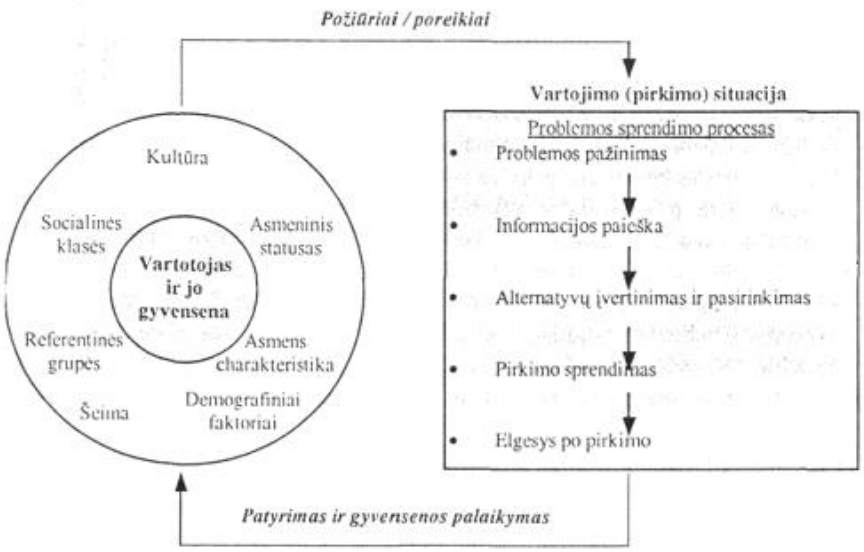
Mano manymu, tokių paslaugų teikimas Lietuvoje yra naujiena, kuria ateityje naudosis ne tik pavieniai asmenys, bet ir firmos, kurios supras, kad joms labiau apsimoka savo kompiuterių apsaugos sistemos testavimą patikėti firmai, kuri nuolat specializuojasi tuo klausimu, o ne samdyti atskirą žmogų, juo labiau, kad tai reikalauja didesnių sąnaudų.

Internetu teikiamos paslaugos, kurios tikrina kompiuterio saugumą yra ne tik nauja Lietuvoje, bet ir labai praktiška. Vartotojui nereikia didelių laiko sąnaudų, jis užsiregistruoja Internetu ir toliau jo kompiuterio saugos testavimu rūpinasi “PC Security” darbuotojai.

Taip pat darbe bus tiriama vartotojų pasinaudojusių “PC Security”, įvertinimo analizė. “PC Security” užtikrina, kad vartotojų duomenys, o taip pat ataskaitos ar kiti konkretaus vartotojo duomenys nebus platinami tretiems asmenims.

Tam, kad įgyti vartotojų pasitikėjimo, turės būti skiriamas didelis dėmesys į klientų poreikių patenkinimą ir tokiu atveju labai svarbi vartotojų elgsena prieš testuojant sistemą ir veiksmus atsiradusius atlikus apsaugos sistemų įvertinimą.

Vartotojų elgsena - tai veiksmai, susiję su paslaugos įsigijimu ir nukreipti į vartotojų norų, poreikių tenkinimą. Iki sprendimo priėmimo ar naudotis sistema ir, ar diegti papildomas paslaugas, klientas mąsto, planuoja, skaičiuoja, tariasi, remiasi patirtimi, ir tik tada priima sprendimą.



pav. 3.2. *Vartotojų elgesio modelis (remiantis H. W. Berkmanu)*

Sprendinių priėmimo požiūriu į problemos sprendimą yra žiūrima labai racionaliai. Tai vartotojas daro remdamasis patirtimi, psichologijos bei ekonomikos pažinimu. Remiantis šiuo požiūriu, pirkinio įsigijimo metu vartotojo pereinami tokie etapai:

- problemos pažinimas;
- informacijos paieškos;
- alternatyvų įvertinimas ir pasirinkimas;
- paslaugos diegėjų pasirinkimas ir užsakymas;
- įvertinimas po diegimo.

3.6. Projekto reikalavimai kokybei

3.6.1. Reikalavimai sistemos išvaizdai

Kad vartotojo neperkrauti papildoma informacija ir koncentruoti dėmesį į sistemos iškeltus uždavinius, svetainėje neturi būti naudojamas gausus grafikos apipavidalinimas ar judantys paveikslėliai. Stiliai turi būti aiškūs ir įskaitomi kiekvienam vartotojui. Kadangi sistema bus naudojamasi interneto naršyklės pagalba, tai jos išvaizda dalinai priklausys ir nuo vartotojo naudojamos naršyklės versijos ir gamintojo, taip pat galimas minimalus skirtumas naudojant

skirtingą monitoriaus raišką. Pagrinde sistemos išvaizda priklausys nuo interneto svetainės dizaino, spalvų, stilių ir grafikos panaudojimo galimybių suderinamumo.

3.6.2. Reikalavimai pakartotiniam panaudojamumui

Nėra sudėtinga panaudoti programuojamos sistemos atskiras bylas ar funkcijas, kadangi programinis kodas dažniausiai nėra pasikartojantis, o tiesiog įtraukiamos nuorodos (įterpimai) į reikiamas programines dalis. Programuojama atsižvelgiant į internetinių sistemų aprašymo principus, taip paprasčiau leidžiant suprasti programinį kodą ne pirminiams programos kūrėjams.

Sistema yra nesudėtinga naudotis ir pradedantiems vartotojams, ir įgudusiems vartotojams. Svetainėje yra surinktos nuorodos į galimai dominančią informaciją, o taip pat pagalbiniai langai į pagalbinę informaciją vartotojui. Pats sistemos įsisavinimas, pradedančiam vartotojui, neturėtų trukti ilgiau kaip valandą nuo darbo su sistema pradžios.

3.6.3. Reikalavimai sistemos veikimui

Sistema nereikalauja ypatingų, jos veikimą tenkinančių, sąlygų. Paprasčiausiai vartotojui reikalingas personalinis kompiuteris su interneto ryšiu ir Interneto naršykle.

Kuriamos programų sistemos, kliento dalies, rekomenduojami minimalūs techninės įrangos reikalavimai:

- procesoriaus taktinis dažnis: >100 MHz
- operatyvinės atminties dydis: > 32 MB
- vaizduoklis: pakankamai didelė skiriamoji geba ir įstrižainė.

3.6.4. Reikalavimai sistemos priežiūrai

Sistemos prižiūrėtojas (Administratorius) turėtų reguliariai peržiūrėti veikimą, turinį ir kreipti dėmesį į vartotojų atsiliepimus bei pastabas. Su laiku pildantis sistemos duomenų bazei, sistemos tvarkytojas, turėtų vis papildyti, o ir senstant informacijai - atnaujinti elektroninės testavimo sistemos informacinę medžiagą. Patarimai ir įsikišimai neturėtų varginti ar nesuprantamai informuoti vartotojo. Taip pat būtinas paslaugumas ir skubus iškilusių problemų sprendimas, norint išlaikyti lojalius vartotojus.

Programų sistema turi būti suprojektuota taip, kad turima informacija negalėtų būti kopijuojama be autorių ar svetainės administratoriaus leidimo. Tokia informacija, kaip duomenų bazės, kitokie sistema besinaudojančių vartotojų parametrai apskritai neturi būti prieinami ir platinami bet kokiam sistemos vartotojui, išskyrus pačius administratorius, kurie taip pat turi

laikytis teisinių ir moralinių įsipareigojimų. Tai turi būti paminėta svetainėje. Skelbiamos nuorodos ir kita medžiaga, aprašymai, komentarai ir kitokie straipsniai turi atitikti visuomenei skelbiamos informacijos reikalavimus.

3.7. Architektūros sprendimas

Projektuojant siekiama sukurti kiek galima lankstesnę sistemą, kurią būtų galima nesunkiai išplėsti papildant naujomis vizualizacijos ar funkcionalumo galimybėmis. Siekiant anksčiau paminėtų tikslų didelis dėmesys bus skiriamas tam, kad kuriama sistema būtų patikima ir saugi.

3.8. Projekto finansiniai klausimai ir gyvavimo laikas

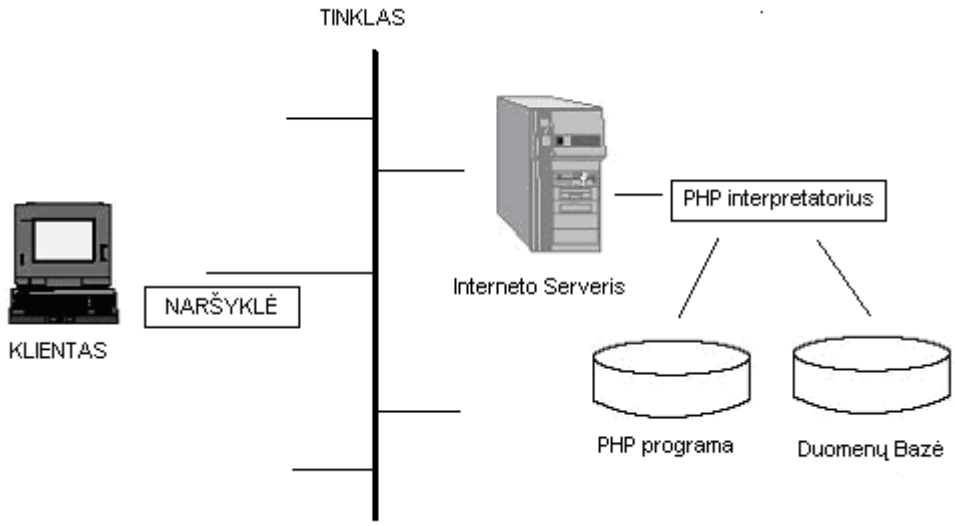
Projekto finansavimas nenumatytas ir šiuo atveju sistema kuriama mokymosi tikslais, pasiliekant teisę ateityje ją įgyvendinti komercinėje srityje. Esant tokiam poreikiui, galima šią sistemą panaudoti ir komerciniams tikslams, panaudojant tuos pačius suprojektuotus modelius – dalis ir papildant sistemą, ją populiarinančiomis priemonėmis.

Konkretus šios programų sistemos gyvavimo laikas nėra numatomas, nes pati sistema yra dalis to, kas mūsų aprašomos sistemos požiūriu bus naudojama netolimos ateities informacinėse sistemose visokeriopai informuojant, padedant vykdyti testavimus, išsaugant nepažeistus duomenis, o tuo pačiu išlaikant vartotoją lojaliu. Esant populiarumui bei sistemos poreikiui esamu metu, svetainės gyvavimas gali būti pratęstas neribotam laikui ir panaudotos svetainės populiarinimo priemonės. Svetainė turi būti pastoviai prižiūrima bei pateikiama informacija atnaujinama.

4. Apsaugos sistemos testavimo projektavimas

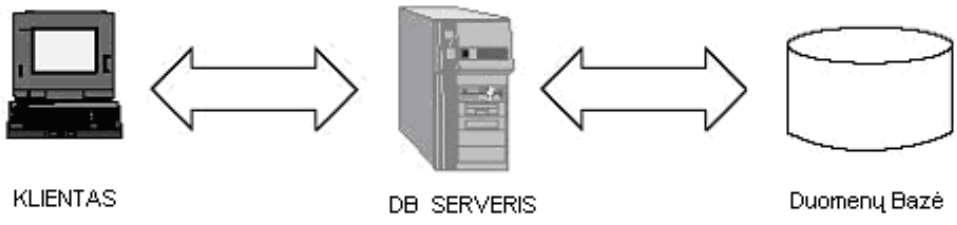
4.1. Bendra interneto serverio funkcionavimo schema

Vartotojui turinčiam interneto naršyklę ir naršant po svetainę, vykdomas toks scenarijus: interneto serveris pateikia užklausą PHP kalbos interpretatoriui, kuris savo ruoštu kreipiasi į duomenų bazę ir atlikęs scenarijaus užduotį grąžina rezultatą vartotojui (atgaliniu keliu) jau kaip HTML internetinį puslapį, atitinkantį vartotojo užklausos rezultatą.



4.1. pav. *Bendra interneto serverio komunikavimo schema*

Interneto serverio architektūra aprašoma panašiais principais kaip ir kliento-serverio architektūra. Paprastai egzistuoja dviejų lygių ir trijų lygių kliento-serverio architektūros (pavaizduota 4.2. pav.).



4.2. pav. *Kliento/serverio architektūra*

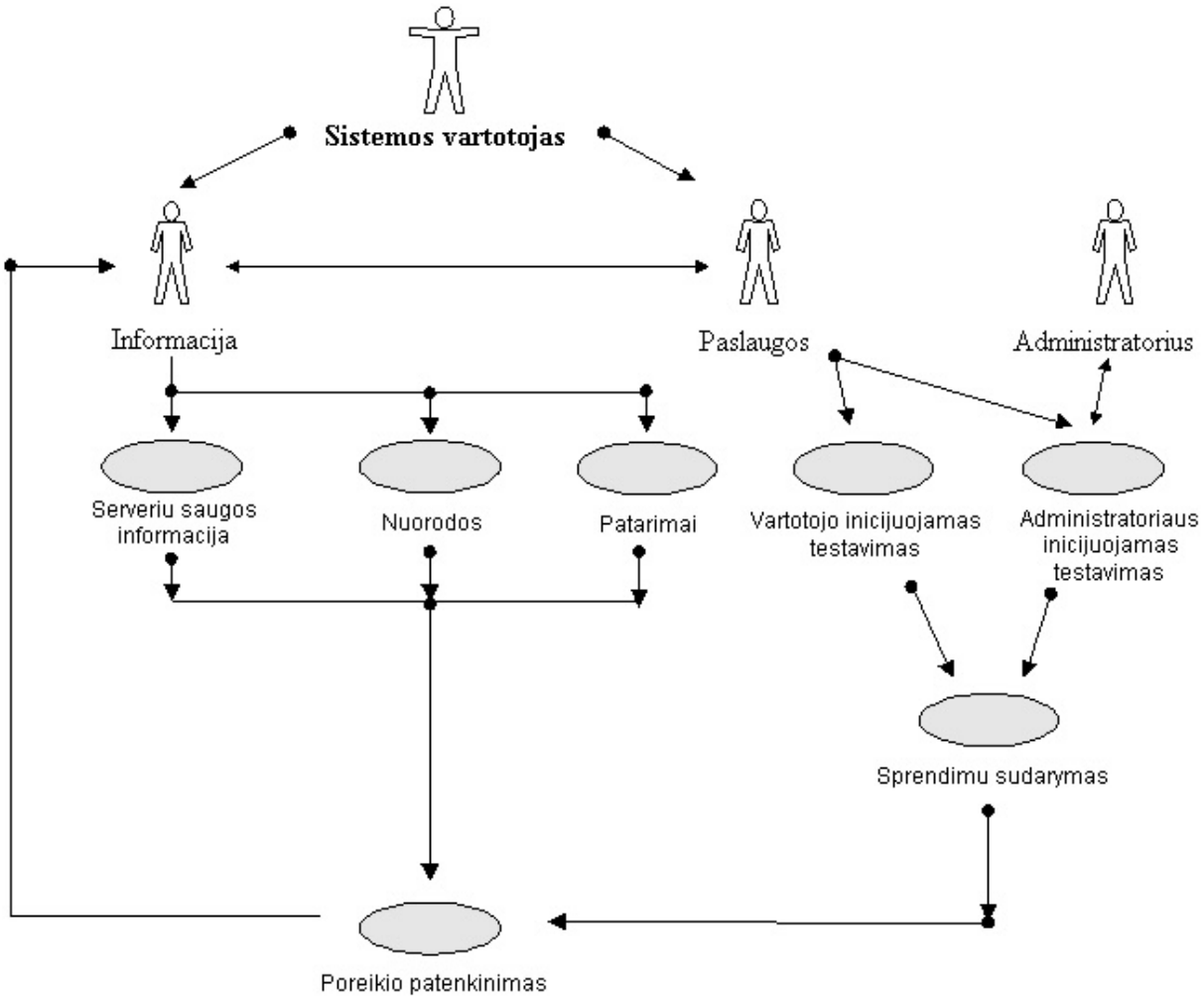
Dviejų lygių kliento-serverio sistemos architektūrą sudaro klientinė pusė kompiuteris su naršykle ir antrinis interneto serveris. Interneto serveris yra sujungtas su duomenų baze ir teikia klientinei pusei informaciją pagal duodamas užklausas. Vartotojas naudodamasi grafine

vartotojo sąsaja mato jau išvestus rezultatus. Trijų lygių architektūroje papildomai yra įterpiamas atskiras duomenų bazių serveris.

4.2. Programos eigos scenarijus, bendra sistemos veikimo schema

Projektuojamai sistemai sukurtas vartotojų prisijungimo ir svarbių duomenų bei informacijos pateikimo programinis modelis, kurį atspindi žemiau esantis programos eigos scenarijus (4.3. pav.).

Iš pradžių vartotojas, prisijungęs prie sistemos, (adresu www.meet.serveriai.lt/security) patenka į pirminį langą, kuriame vienoje pusėje matomi meniu punktai, viduryje – informacija, kitoje – registruotų vartotojų prisijungimo laukeliai. Programos eigos scenarijus gali būti atvaizduotas taip:



pav. .4.3. *Programos eigos scenarijus*

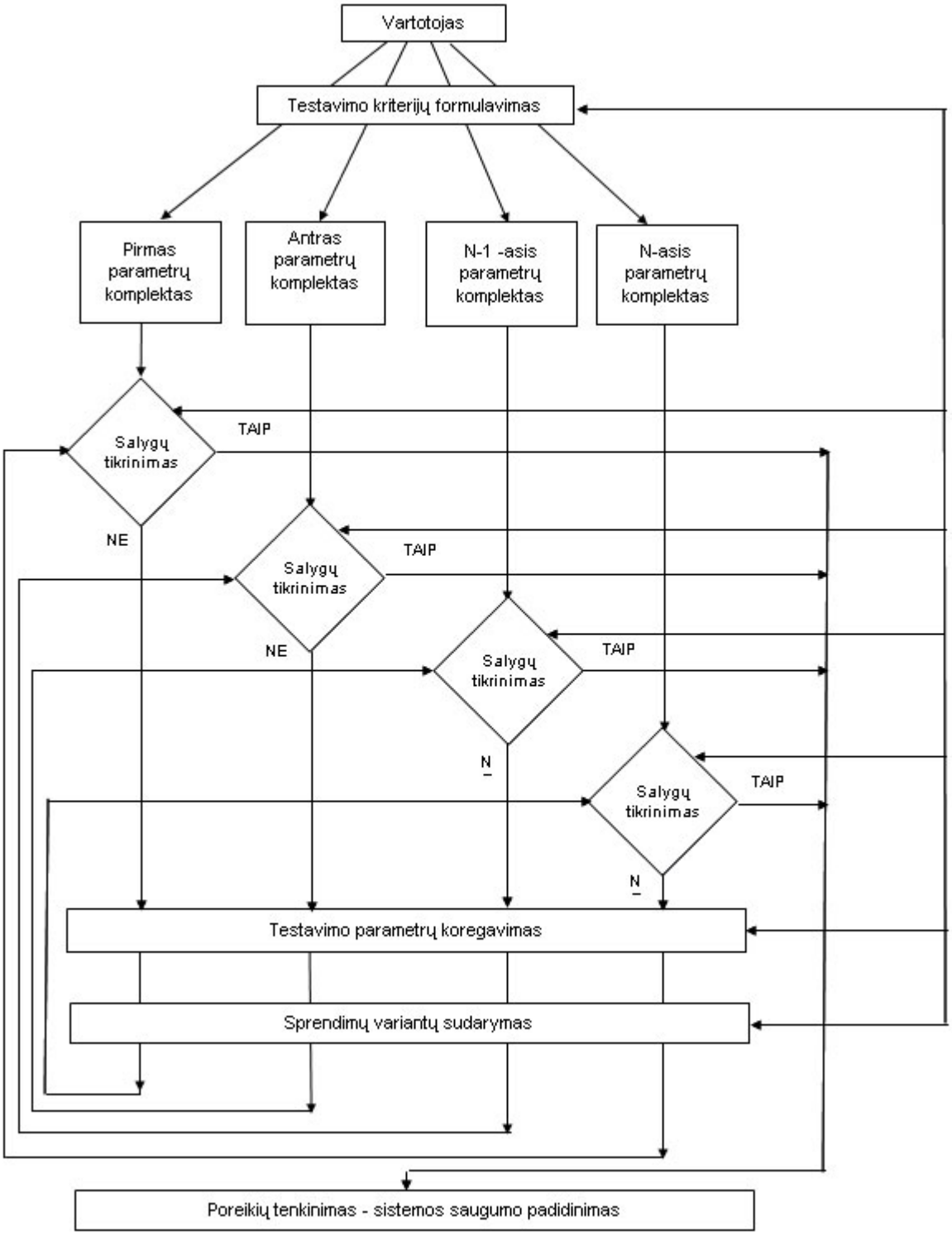
Norėdamas pradėti naudotis sistema, fizinis ar juridinis asmuo, pradžioje turi užsiregistruoti – t.y. užpildyti svetainėje esančią formą ir, administratoriui patvirtinus jo prašymą, gauti priėjimą prie sistemos – vartotojas gaus asmeninius prisijungimo parametrus.

Suvedęs savo prisijungimo duomenis ir papildomai išvestą saugaus prisijungimo slaptažodį, registruotas vartotojas patenka į sistemą.

Sekančiame etape vartotojas gali nustatyti, kokiu būdu jis pageidauja, kad jo tinklo kompiuterius ar konkrečiai tik jo kompiuterį tikrintų ši interneto serverių apsaugos sistemų testavimo programa. Ji gali būti realiu laiku inicijuojama pačio vartotojo arba paliekant žinutę-užsakymą, kad tai atliktų sistemos administratorius.

Atlikus testavimą yra sukuriamos ataskaitos ir pagal jas gali būti siūlomi sprendimai kaip išspręsti esamas apsaugos sistemos problemas. Jei norima pasirinkti sistemos testavimą pagal kitus kriterijus – procedūra vykdoma iš naujo sužymint (ar įvedant) kitus parametrus.

Žemiau pateikiama interneto serverio apsaugos testavimo sistemos bendra veikimo schema (4.4. pav.):



4.4. pav. *Bendra sistemos veikimo schema*

4.3. Interneto serverio, duomenų bazės sutrikimai

Projektuojamos sistemos funkcionavime gali pasitaikyti trijų tipų veikimo sutrikimai:

- Interneto serverio sutrikimas;
- Duomenų bazės sutrikimas;
- Programinė sistemos klaida.

Interneto serverio sutrikimo atveju (pvz., serveris yra administratoriaus laikinai sustabdytas ar kitos nuo administratoriaus nepriklausomo priežastys), vartotojams sistema tokiu atveju bus nepasiekiama. Šiuo atveju sistemos vartotojams teks palaukti, kol Interneto serverio administratorius atstatys Interneto serverio funkcionavimą. Po Interneto serverio atstatymo, sistema toliau sėkmingai tęs savo darbą.

Duomenų bazės (lokalios ar bet kurios nutolusios) sutrikimo atveju (pvz., DBVS yra administratoriaus laikinai sustabdyta, arba serveris laikinai išjungtas), pati apsaugos sistemos testavimo svetainė galės pateikti ir išanalizuoti užklausas, tačiau sprendimo variantų peržiūrėti negalės dėl duomenų nepasiekiamumo. Vartotojams tokiu atveju bus suformuluojamas klaidos pranešimas. Atsiradus ryšiui su duomenų baze, pakeitimų joje neturėtų būti ir atstatomas sėkmingas veikimas.

4.4. Sistemos UML specifikacija

Šiuolaikinių programų sistemų struktūra ir elgsena neretai tampa labai sudėtingos. Jų projektavimas pasižymi tokiomis savybėmis kaip daugiasluoksnė architektūra, smulkios detalizacijos klasių struktūros, paskirstymas, lygiagretumas, sugebėjimas reaguoti į išorės veiksnius ir pan. Gauta programinės įrangos architektūra turi tenkinti sistemų palaikomumo ir konfigūravimo reikalavimus. Objektinio modeliavimo principas įgalina sistemiškai abstrahuoti ir (de)komponuoti tokios sistemos savybes. Šį principą palaikantys modeliavimo įrankiai leidžia transformuoti šias savybes į atitinkamus objektinės struktūros ir elgsenos modelius.

Faktiniu standartu objektinio modeliavimo srityje pripažinta UML (*Unified Modeling Language*). Šios kalbos notacija leidžia grafiškai atvaizduoti sistemos reikalavimus, struktūrą ir elgseną, nepriklausomai nuo sistemos realizavimo specifiškumų. Be to, UML pirmiausiai vis tik yra vizualinio specifikavimo kalba, daugeliui specifikacijų naudojanti diagramas. Tai labai svarbu aprašant sudėtingus sąryšius, kurie retai turi paprastą nuoseklią struktūrą ir yra sunkiai aprašomi paprastu tekstu. Dažnai lygiagrečiais tampantys valdymo srautai, skirtingi vaidmenys ir jų įgaliojimai, resursų būsenų pokyčiai itin svarbūs bandant suprasti sistemos elgseną, ir juos būtina išreikšti vizualiai. Sistemos modeliavimui struktūriniu požiūriu objektiniame modeliavime buvo pritaikytas vienintelis – esybių-ryšių – modelis, kuris įvairiose metodologijose skiriasi nebent grafiniais žymėjimais. Tuo tarpu elgsenai modeliuoti yra taikomi keli iš esmės skirtingi modeliai. Bendradarbiavimo modeliavimui, kuris orientuotas į vaidmenis ir jų sąveikas, reikalingas vykdant užduotis, skirtos bendradarbiavimo (*collaboration*) ir sekų (*sequence*)

diagramos; veiklos (*activity*) ir būsenų (*statechart*) diagramos vaizduoja sistemos reakcijas į veiksnius.

4.4.1. Bendras sistemos modelis

Projektuojamai internetinių serverių testavimo sistemai kuriamas sistemos modelis UML kalba.

Sistemos modelis (UML kalba) sudaromas iš tokių abstrakcijos lygių:

- naudojimo modelio (angl. *Use Case, 4.4.2. skyrius*),
- loginio modelio (angl. *Logical, 4.4.3. skyrius*),
- ir sistemos komponentų modelio (angl. *Component, 4.4.4. skyrius*),

4.4.2. Naudojimo modelis

Naudojimo modelis padeda geriau suprasti sistemos taikymo sritį.

Čia veikiantys objektai vaizduojami, kaip žmogeliukai, o taip pat atvaizduojamos ir jų būsenos, procesai ir visi kiti informacijos mainai. Naudojimo modelis paprastai susideda iš keturių tipų diagramų:

- naudojimo atvejų diagramų,
- būsenų diagramų,
- veiksmų sekų diagramų,
- bendradarbiavimo diagramų.

El. asistento sistemos naudojimo modelis susideda iš:

Naudojimosi atvejų:

- visi vartotojai (*pav. 4.6.*),
- administratoriaus režimas (*pav. 4.7.*),
- pagrindinė (angl. *main*) diagrama (*pav. 4.8.*).

Būsenų (angl. *state*) diagramų:

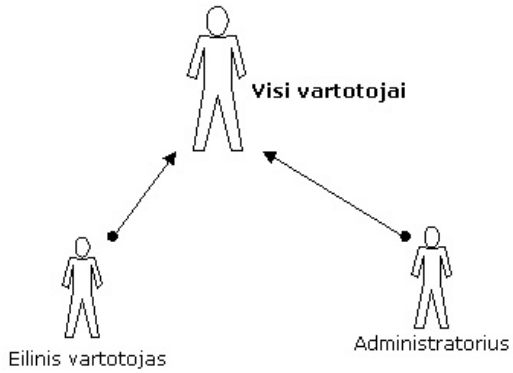
- eilinio vartotojo būsenos (*pav. 4.9.*),
- administratoriaus būsenos (*pav. 4.10.*).

Bendradarbiavimo (angl. *collaboration*) diagramos:

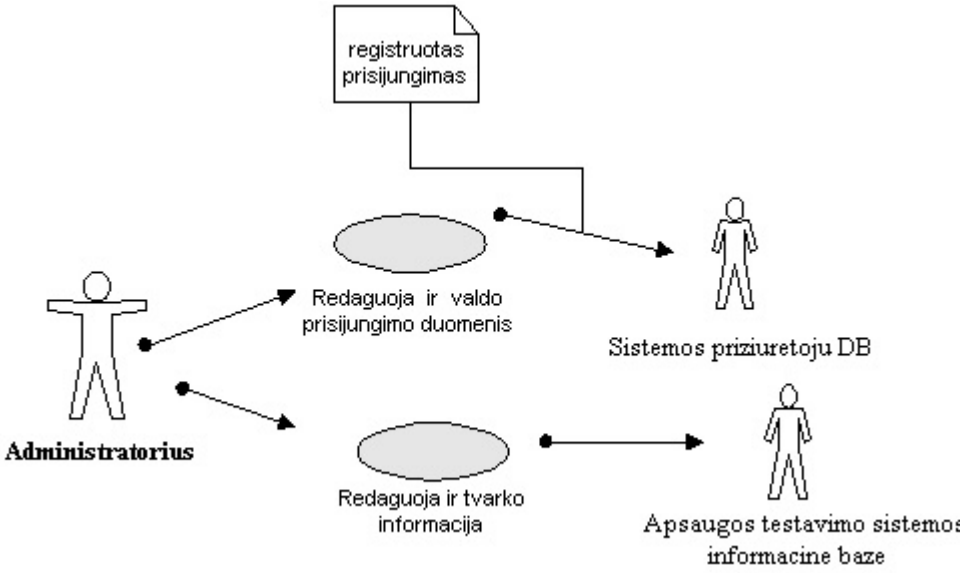
- apsaugos testavimo sistemos veikimo principas (*pav. 4.11.*).

Veiksmų sekų (angl. *sequence*) diagramų:

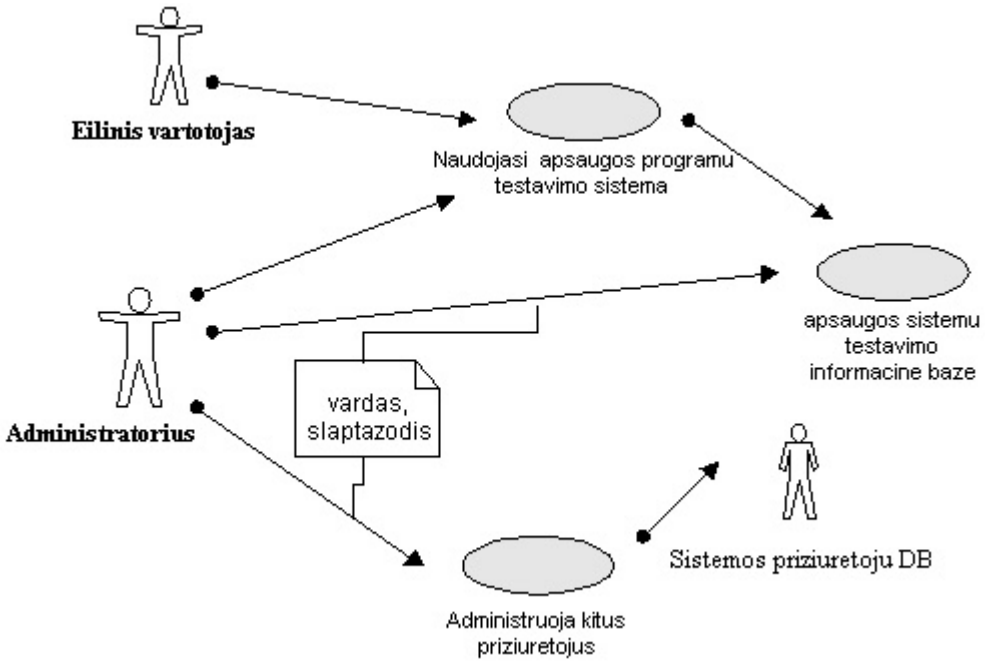
- informaciniai mainai sistemoje (*pav. 4.12.*).



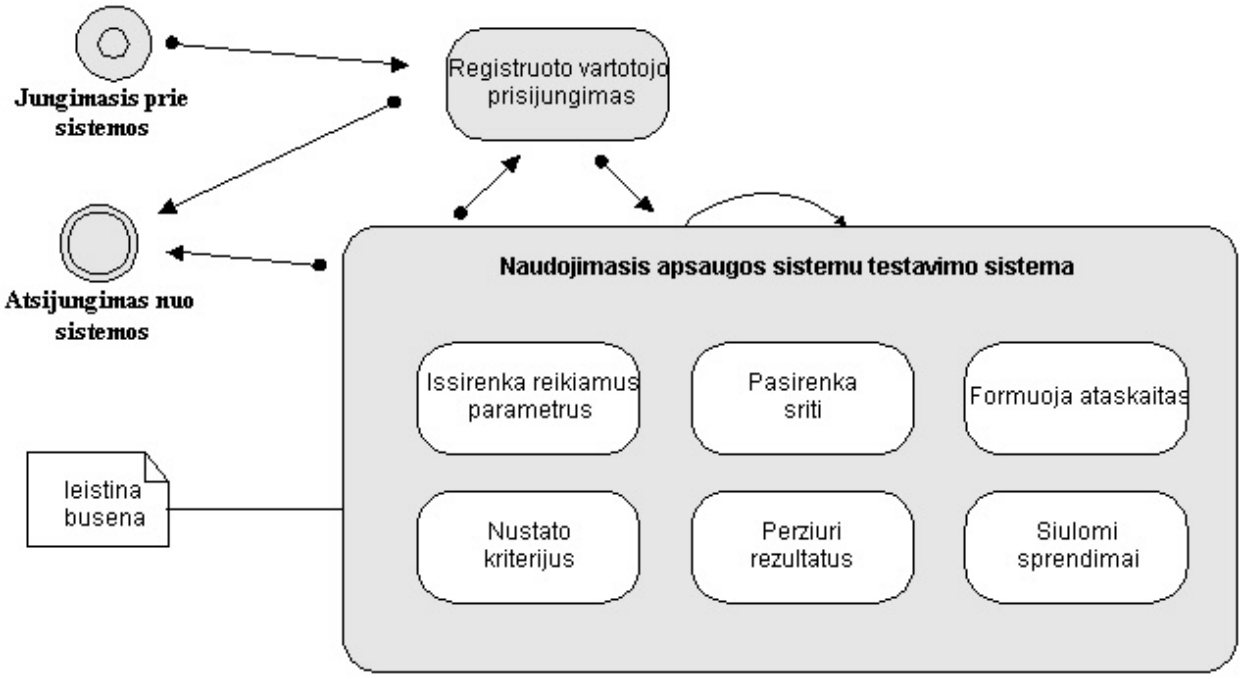
pav. 4.6. Visi vartotojai



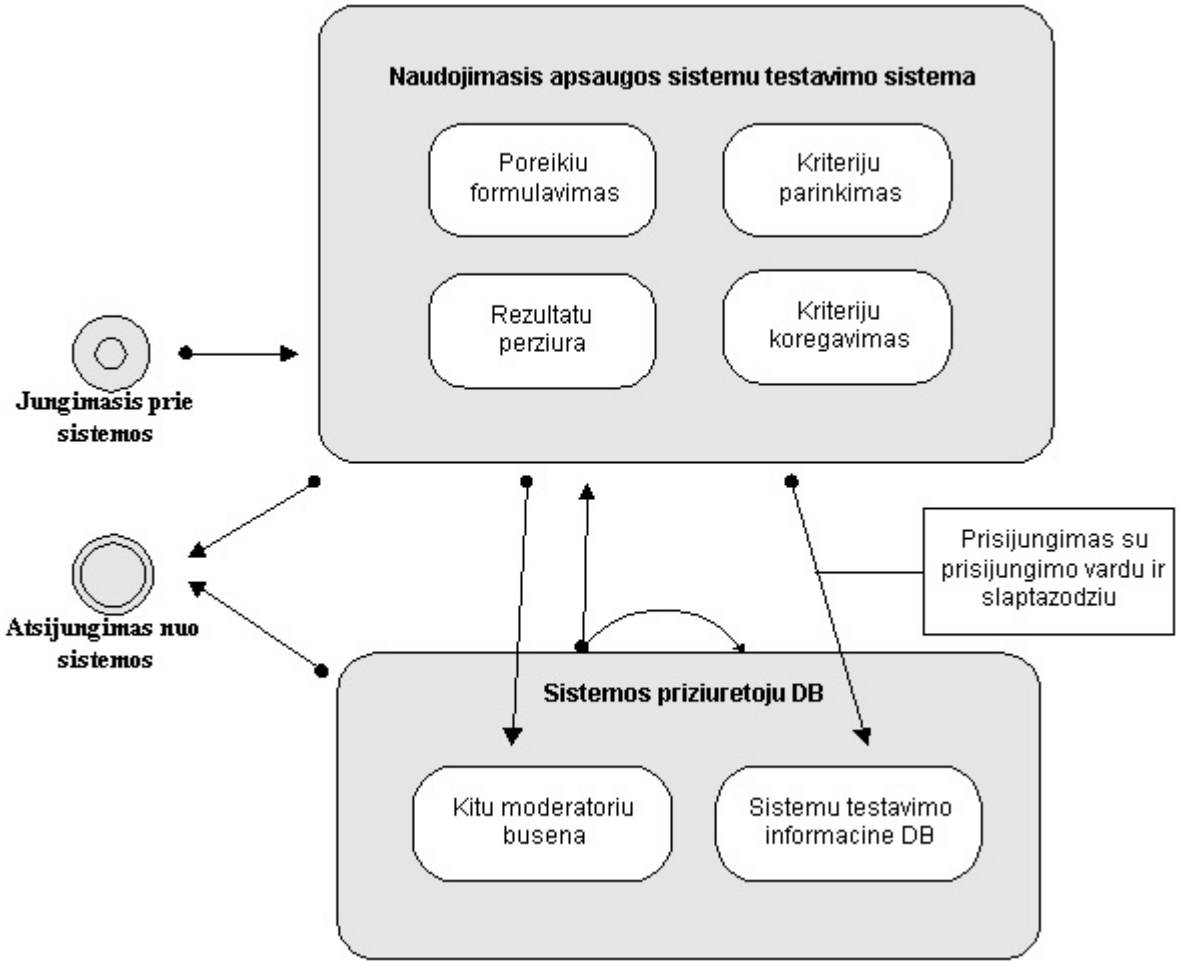
pav. 4.7. Administratoriaus režimas



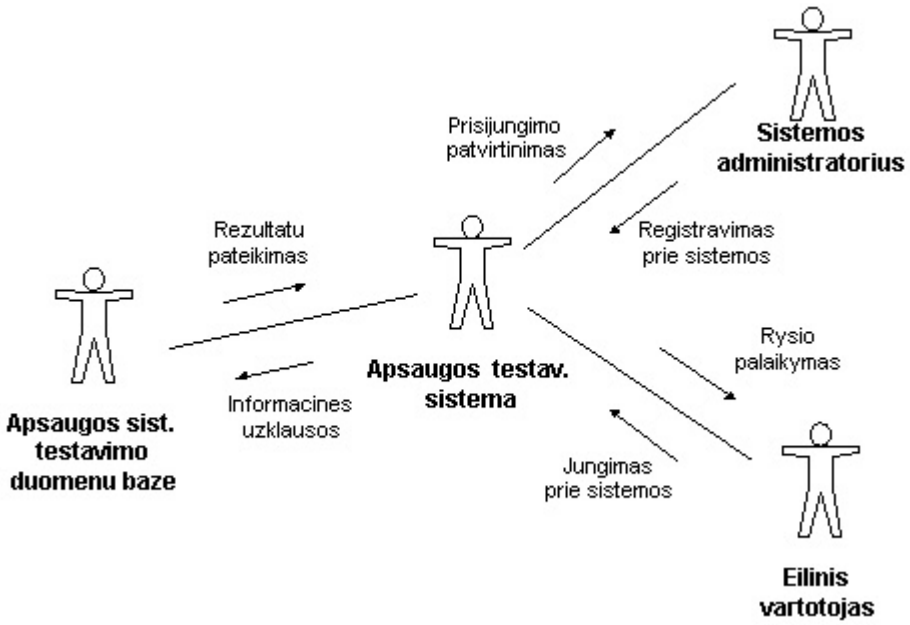
pav. 4.8. Pagrindinė diagrama



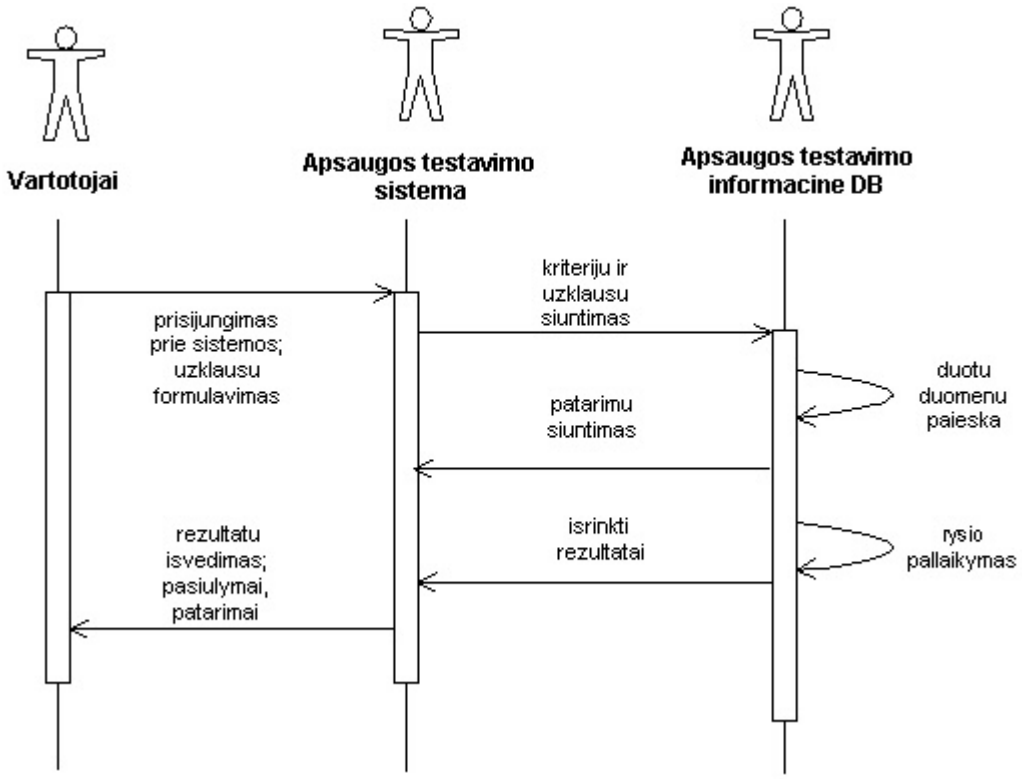
pav. 4.9. Registruoto vartotojo būsenos



pav. 4.10. Administratoriaus būsenos



pav. 4.11. Apsaugos testavimo sistemos veikimo principas



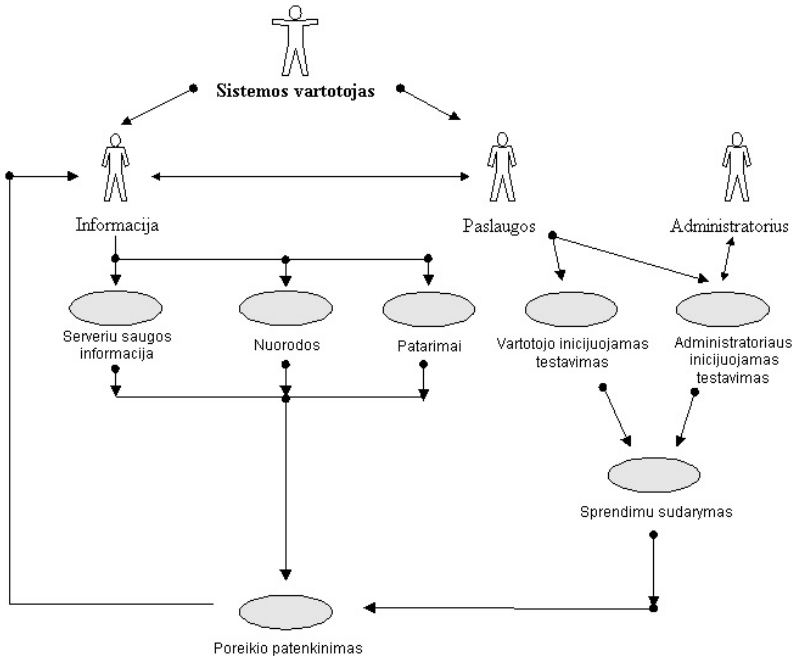
pav. 4.12. Informaciniai mainai sistemoje

4.4.3. Loginis modelis

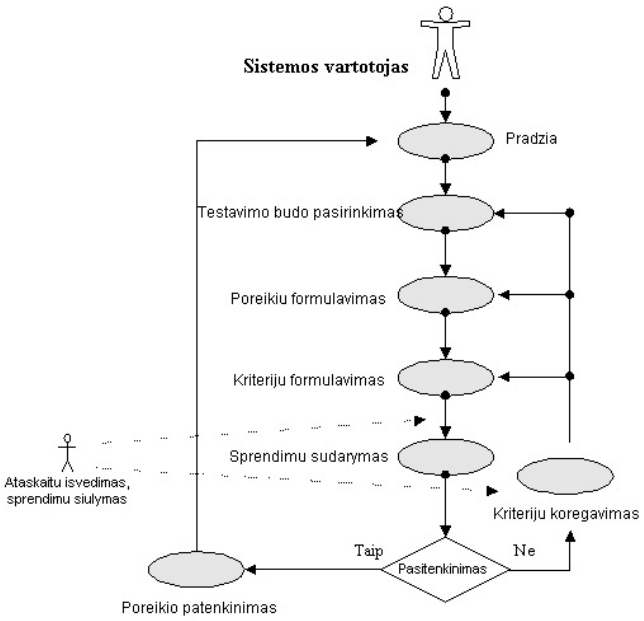
Loginis modelis atspindi sistemos funkcinius reikalavimus. Šį modelį sudaro duomenų bazės lentelės ir ryšiai tarp jų.

Sistemą sudaro šios diagramos:

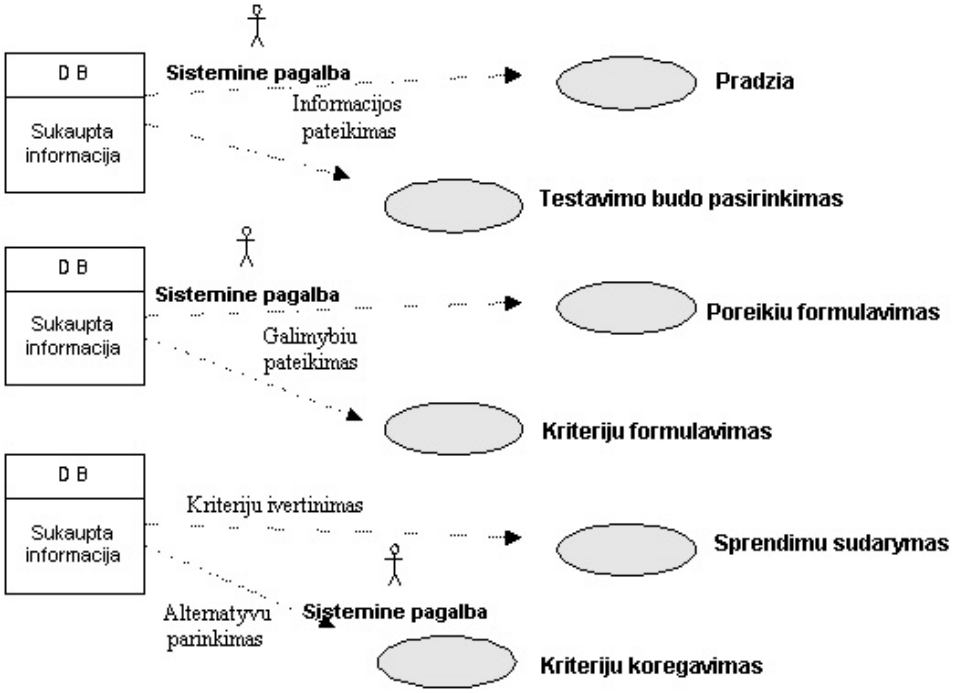
- bendra sistemos eigos schema (*pav. 4.13.*).
- apsaugos testavimo sistemos būsenų diagrama (*pav. 4.14.*).
- apsaugos testavimo sistemos veikimo struktūros diagrama (*pav. 4.15.*).
- pagrindinė duomenų srautų (angl. *main*) diagrama (*pav. 4.16.*).



pav. 4.13. Bendra sistemos eigos schema



pav. 4.14. Apsaugos testavimo sistemos būsenų diagrama



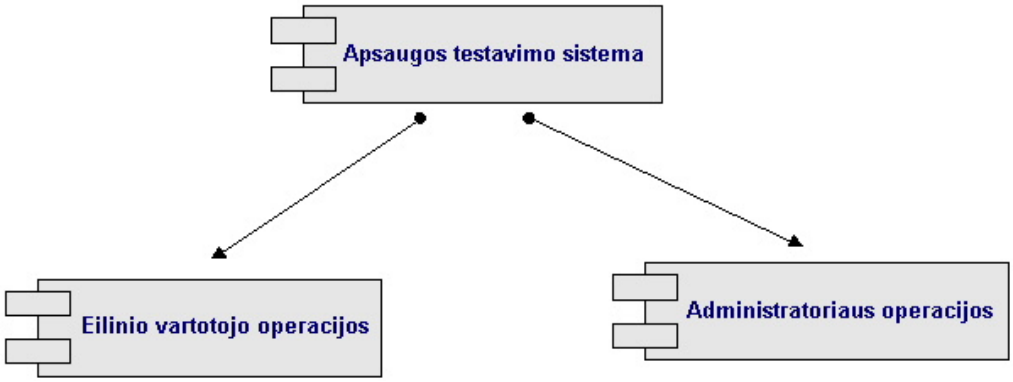
pav. 4.15. Apsaugos testavimo sistemos struktūros diagrama

4.4.4. Sistemos komponentų modelis

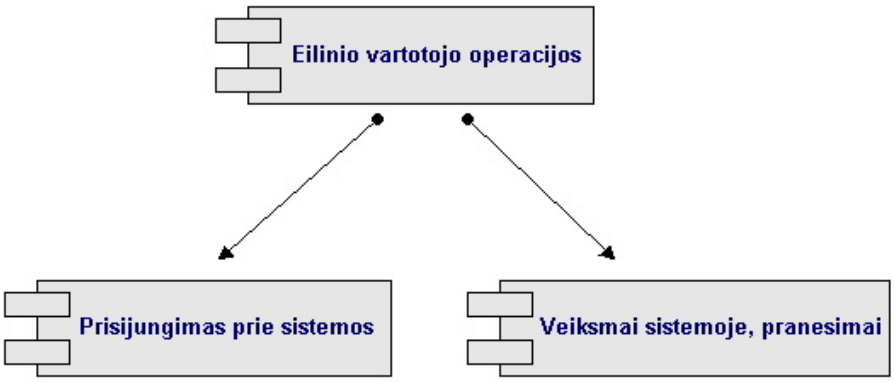
Sistemos komponentų modelis nusako sistemos modeliškumą, failų ir servisų pasiskirstymą.

Sistemos komponentų modelis sudarytas iš šių diagramų:

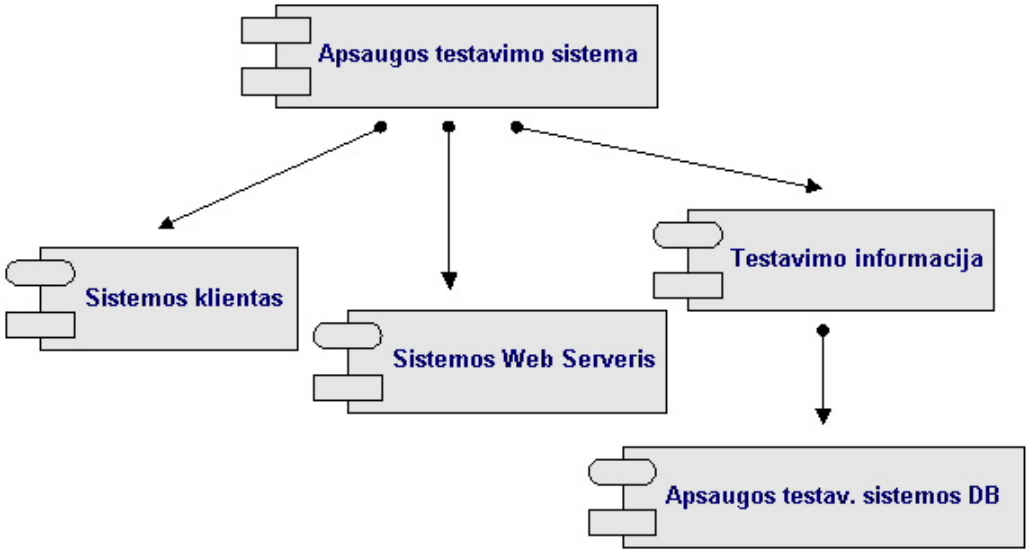
- sistemos funkcijų diagrama (*pav. 4.17.*),
- eilinio vartotojo funkcijų diagrama (*pav. 4.18.*),
- kliento-serverio funkcijų diagrama (*pav. 4.19.*).



pav. 4.17. Sistemos funkcijų diagrama



pav. 4.18. Eilinio vartotojo funkcijų diagrama



pav. 4.19. Kliento-serverio funkcijų diagrama

5. Interneto serverių apsaugos sistemos aprašymas

5.1. Techninis pasiūlymas

5.1.1. Sistemos paskirtis

Sparčiai tobulėjant informacinėms technologijoms, vis daugiau tiek fizinių, tiek juridinių vartotojų jungiasi į bendrą pasaulinį kompiuterių tinklą - Internetą. Vieni jungiasi bendravimo tikslais, kiti paprasčiausiai negali be jo apsieiti, nes tai neatsiejama jų darbo dalis. Daugėjant Interneto vartotojų skaičiui, daugėja ir tokių žmonių dalis, kurie bando vienaip ar kitaip patekti į kito vartotojo kompiuterį savanaudiškais, dažnai padarančiais nemažai žalos, tikslais. Tai įgyvendinama pasinaudojus silpnosiomis sistemos vietomis, todėl norint, kad įsilaužėlis rastų kuo mažiau spragų kito asmens kompiuterio sistemoje, reikia nuolat rūpintis jos saugumu, kiek galima labiau pašaliniams uždaryti visus priėjimo kelius prie savo kompiuterinės sistemos.

5.1.2. Pagrindinės sistemos funkcijos, funkciniai reikalavimai

- Mūsų duomenų bazė turi saugoti firmos mums patikėtus jos esamus IP adresus, skenavimo ataskaitas bei turi būti galimybė juos redaguoti.
- Interneto portalas, su nmap programos pagalba, turi praskenuoti šiuos IP adresus, patikrinant, kurie prievadai yra atviri bei mažinantys sistemos saugumo lygį.
- Iš gautų rezultatų turi būti sudaromos ataskaitos. Jos turi būti pateikiamos su nuorodomis į informaciją apie esamos problemos sprendimo būdus.
- Šios ataskaitos su papildoma informacija turi būti koduojamos ir saugiai persiunčiamos vartotojams jų nurodytu adresu.

5.1.3. Reikalavimai techninei ir programinei įrangai

- Vartotojo bei sistemą „palaikantys“ kompiuteriai: rekomenduotini galingesni nei Pentium 100MHZ, 32 RAM;
- Programų sistemos kūrimo priemonės: MySQL, HTML, PHP, JavaScript programavimo kalbos;
- Naršyklės: internet Explorer 5 ir naujesnės versijos bei analogiškos kitų gamintojų naršyklės.

- Techninė įranga. Mūsų Interneto serveris turi būti įdiegtas ant Intel Pentium platformos su pakankamais atminties ir mikroprocesoriaus resursais
- Interneto serverio programinė įranga – Apache 2.0. Binarinė šio serverio instaliacinė versija veikia tik su x86 šeimos procesoriais Intel ir AMD
- Interneto serverio operacinė sistema – MS Windows 2000 Pro server, Linux
- Naudojama duomenų bazė – MySql
- Papildoma programinė įranga: mūsų Interneto portalas bus parašytas naudojant PHP programavimo kalbą. Kliento hostai bus skenuojami Nmap programa

5.1.4. Projektavimo resursai ir priemonės

Kaip pagrindinės priemonės – projektavimui ir programavimui naudojama asmeninio kompiuterio, kaip serverio, duomenų bazių valdymo sistema MySQL, ir PHP internetinių puslapių programavimo priemonės, kitos laikinam išbandymui bei programavimo darbus palengvinančios (*shareware* bei *freeware*) programinės įrangos priemonės, asmeninė literatūros biblioteka.

5.2. Funkcinė specifikacija

5.2.1. Produkto vartotojai, tipai

Paslauga gali naudotis kiekvienas, mokantis dirbti kompiuteriu, tačiau darbas bus efektyvesnis, jei vartotojas turės bent minimalias žinias apie taikomąją sritį.

Vartotojams būtinos lietuvių kalbos žinios. Programa yra skirta lietuviškai kalbančių vartotojų grupei, todėl visi paaiškinimai pateikiami būtent šia kalba.

Skiriamos dvi vartotojų grupės: klientai ir Interneto portalo administratorius.

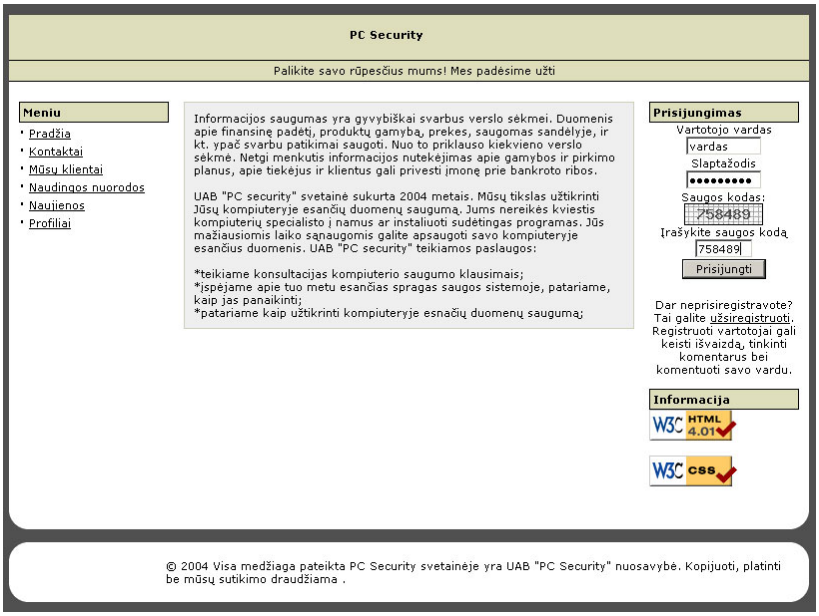
Klientai: tai organizacijos, firmos ar pavieniai asmenys, kurių kompiuteriai yra prijungti prie Interneto. Klientų problemų apibūdinimas: kadangi absoliučiai saugių sistemų nėra, tai siekiama pažeidžiamų sistemos vietų skaičių sumažinti iki minimumo, kad įsilaužėlis negalėtų patekti į organizacijos kompiuterinę sistemą. Priešingu atveju, gali būti pavogta, pakeista ar įmonės konkurentams perduota svarbi informacija, ko pasekoje, klientas patirtų mažesnius ar didesnius moralinius ir materialinius nuostolius**.**

Interneto portalo administratorius: tai asmuo atsakingas už patikimą paslaugos teikimą. Administratorius privalo suprasti esamą saugos svarbą, turi turėti atitinkamas žinias apie galimas sistemos silpnąsias vietas bei jų sprendimo būdus.

5.2.2. Sistemos vartotojo specifikacija

5.2.2.1. Prisijungimas prie svetainės

Iš pradžių vartotojas, prisijungęs prie sistemos, (adresu www.meet.serveriai.lt/security) patenka į pirminį langą, kuriame vienoje pusėje matomi meniu punktai, viduryje – informacija, kitoje – registruotų vartotojų prisijungimo laukeliai. Pirminis programos langas atrodo atvaizduojamas taip:



a. **pav.** Pirminis programos langas

Vartotojo sąsaja suderinta su šiomis interneto Internet Explorer versija 5 bei analogiška arba kitomis HTML 4.0 standartą palaikančiomis naršyklėmis.

5.2.2.2. Dominančios srities informacija

Spaudžiant dominančios informacijos srities mygtuką (tesktas su užrašu) „Naudingos nuorodos“ ir atitinkamai kitus, papuolama į puslapį, kuriame ir patalpinta norima informacija. Čia surinkta informacija padės

vartotojams greičiau susiorentuoti svetainės paslaugų pasiūloje, taip pat peržvelgti tos pačios srities svetainių turinius.

5.2.2.3. Prisijungimas prie apsaugos sistemų testavimo

Norėdamas pradėti naudotis sistema, fizinis ar juridinis asmuo, pradžioje turi užsiregistruoti – t. y. užpildyti svetainėje esančią formą ir administratoriui patvirtinus jo prašymą gauti priėjimą prie sistemos – vartotojas gaus asmeninius prisijungimo parametrus.

Suvedęs savo prisijungimo duomenis ir papildomai išvestą saugaus prisijungimo slaptažodį registruotas vartotojas patenka į sistemą.

Sekančiame etape vartotojas gali nustatyti kokiu būdu jis pageidauja, kad jo tinklo kompiuterių ar konkrečiai tik jo kompiuterį tikrintų ši interneto serverių apsaugos sistemų testavimo programa. Ji gali būti realiu laiku inicijuojama pačio vartotojo arba paliekant žinutę-užsakymą, kad tai atliktų sistemos administratorius.

Atlikus testavimą yra sukuriamos ataskaitos ir pagal jas gali būti siūlomi sprendimai kaip išspręsti esamas apsaugos sistemos problemas. Jei norima pasirinkti sistemos testavimą pagal kitus kriterijus – procedūra vykdoma iš naujo sužymint (ar įvedant) kitus parametrus.

5.2.3. Sistemos administratoriaus specifikacija

5.2.3.1. Apsaugos serverių testavimo validavimas

Sistemos prižiūrėtojas, jam sankcionuotu prisijungimu, (kitaip administratorius) prižiūri šiose sistemoje naudojamą informaciją, o taip pat vykdo užklausas tų klientų, kurie pageidauja, jog jų sistemų testavimas būtų atliekamas būtent per administratorių. Tokiu atveju administratorius patvirtina užsakovo užklausą, kurio pasekoje, sistema testuoja kliento serverio saugumo spragas. Iš gautų rezultatų suformuojami sprendimai ir, atitinkamai pagal poreikius ir galimybes, administratorius siunčia ataskaitą arba pats įvykdo pataisymus.

Pati papildoma informacija egzistuoja tekstiniu formatu ir redaguojama paprasčiausios užrašinės būdu.

5.2.3.2. Duomenų bazių priežiūra ir redagavimas

Galutiniems sprendimams ir rezultatams išvesti yra panaudojama lokali ar nutolusi duomenų bazė, kur, pateikus atitinkamas užklausas išrenkami taisyklingi duomenys. Priėjimą įsteigti ryšį ir galimybę redaguoti pačią duomenų bazę turi tik sistemos administratorius su jam žinomu prisijungimo vardu ir slaptažodžiu.

5.3. Sistemos apribojimai

Paprastam interneto vartotojui pateikiamas funkcionalumas turi būti prieinamas kuo platesniam vartotojų ratui, t.y. funkcionalumo pateikimo forma turi būti suderinama su dauguma populiarių interneto naršyklių.

Sistemos administratoriaus režimas turi būti patikimai apsaugotas. Pašalinių asmenų patekimas į produkto administravimo sistemą gali reikšti konfidencialios informacijos atskleidimą, sukauptų duomenų sunaikinimą ar klastojimą, todėl yra neleistinas.

- Naudojami standartai: TCP/IPv4 ir HTTPS
- Programinės įrangos apribojimai: kliento Interneto naršyklė turi palaikyti SSL protokolą.
- Klientui siunčiamos ataskaitos bus koduojamos PGP kodavimo sistema

5.4. Vartotojų sąsajos specifikacija

Apibendrinti reikalavimai vartotojo sąsajai esti tokie:

Informatyvi - tai pasiekiama pateikiant informaciją struktūrizuotai, t.y. pvz. duomenų bazės įrašus pateikiame lentele ar išplėstiniu medžiu, taip pat informacija skaidoma į atskirus lygius pagal duomenų klases (naujai įtraukiamos nuorodos, publikuojamos nuorodos ir t.t.);

Intuityvi navigavimo atžvilgiu - visa navigavimo sistema remiasi duomenų struktūrų ryšiais ir savybėmis, pvz., iš bendro „būsto paieškos“ puslapio galima pereiti į „būsto kriterijų formulavimo“ peržiūros ar paieškos puslapį, iš šio - į „rezultatų apdorojimo“ puslapį ir t.t. Tuo pačiu paliekama galimybė grįžti į bet kurį iš puslapių, esančių kelyje iki aktyviojo.

Neperkrauta: nors svetainės turi būti informatyvios ir su gera navigavimo sistema, bet jos taip pat turi būti neperkrautos informacija (tai pasiekiama neišduodant iš karto visos duomenų bazės lentelių informacijos, o ją pateikiant prioritetų (svarbos) žingsniais);

Interneto svetainė turi atitikti ir dizaino rekomendacijas (suderintos, neryškios spalvos, mažesnis informacijos langas, informatyvūs meniu punktai ir pan.).

Turi būti grafinė vartotojo sąsaja, kuri realizuota pagrindiniame meniu, iš kurio galima pasirinkti reikiamas atlikti veiksmus:

Peržiūrėti duomenis savo duomenis.

Peržiūrėti paskutines skenavimo ataskaitas.

Papildyti duomenų bazę naujais įrašais.

Atsispausdinti ar nusiųsti sudominusią naujieną.

Jeigu nustatyta klaida, sistemos vartotojui išvedamas pranešimas apie klaidingų duomenų įvedimą.

Grafiniai duomenys saugomi JPEG, GIF formatu.

5.5. Bendri realizacijai keliami reikalavimai

Produkto patikimumas: sistemos administravimas turi būti neprieinamas pašaliniams vartotojams. Pašalinių vartotojų patekimas į sistemą gali reikšti sukauptos konfidencialios informacijos nutekėjimą, duomenų praradimą (sukurtų vartotojų ir sukauptų duomenų sunaikinimą), bei sistemos administravimo perėmimą. Tokiems įsilaužimams išvengti, būtina naudoti patikimą vartotojo identifikavimo ir vartotojo autorizuotos sesijos valdymo sistemą.

Bendra produkto kokybė: turi būti užtikrinama aukšta produkto kokybė: patogi ir suprantama navigacija, neskurdus, tačiau ir neperkrautas dizainas, galimybė operatyviai peržiūrėti rezultatus, nes sistema bus naudojama kasdieniniame gyvenime. Taigi sistema turi būti patogi ir tuo pačiu paprasta.

Produkto įtaka sistemai, kurioje bus naudojamas: šiuo atveju produktas yra siaurai specializuotas (būsto pasirinkimo konsultavimas), taigi jis nepaveiks visos sistemos darbo, ir minimaliai naudosis sisteminiais resursais, netrikdys kitų kompiuterio vykdomų užduočių. Numatoma sistemą plėsti ir pačioje programos aplinkoje (lokaliai) turėti duomenų bazę, kurioje kaupiama reikalinga informacija.

Numatomas produkto gyvavimo ciklas: konkretus sukurto produkto gyvavimo laikas nėra numatomas. Produkto moralinį senėjimą laikui bėgant galima atsverti funkcionalumo papildymais.

Programinės įrangos mobilumas: galima naudoti visuose kompiuterizuotose darbo vietose, kuriuose įdiegta HTML standartą palaikanti interneto naršyklė.

Kokybiškam darbui svetainės lankytojams rekomenduojama naudoti IE naršykles, nes kitos naršyklės gali šiek tiek iškraipyti sąsają. Taip pat ir administratoriui reikalinga naršyklė, palaikanti HTML 4.0 standartą;

Interneto serveris, kuriame ši svetainė bus įdiegta, turės palaikyti HTML 4.0 standartą, PHP4 programavimo kalbos programas ir privalės turėti ryšį su MySQL bei suderintu su PHP4, duomenų bazės serveriu.

5.6. Reikalavimai saugumui

Nors projekte nėra įgyvendinta finansinių transakcijų, tačiau vartotojui, kaip ir sistemos administratoriui reikia žinoti pagrindinius interneto sistemų saugumui keliamus reikalavimus.

Jau anksčiau interneto sistemų kūrėjai suprato, kad jei norima įgyvendinti verslo procesų modelį internete, reikia kreipti didelį dėmesį į su saugiu duomenų pasikeitimu susijusias problemas. Pagrindinės naršyklės Netscape Navigator ir Microsoft Internet Explorer turi integruotus saugių prisijungimo sluoksnių (*secure socket layer* – toliau SSL) technologiją. Opera naršyklė taip pat jau palaiko šiuos standartus. SSL technologija integruota į daugumą „pirkimo krepšelių“ internetinių svetainių ir kitas sistemas, kur reikalingas elektroninis duomenų patvirtinimo sertifikatas. Šis sertifikatas dar turi *VeriSign* pavadinimą ir daugumoj rimtų interneto svetainių reikalaujama jį turėti. Sertifikatas atstoja „parašą“, kuriuo patvirtinamas saugus prisijungimas prie tam tikros interneto sistemos. Vartotojo vardas, adresas ir svarbūs kreditinės kortelės numeriai yra šifruojami visa eile matematinių kodavimo algoritmų tam, kad užtikrinti tik licenzijuotą prisijungimą prie serverio, kuriam yra tinkama tokia informacija.

Taip pat vartotojams suteikia patikimumo tas faktas, kad interneto transakcijos atliekamos per *https://* vietoj *http://* panaudojimo. Šio prisijungimo standarto naudojimas matomas naršyklės apatiniame kampe atsiradus rakto simboliui. Tokio standarto užkodavimas pripažintas patikimas tiek, kad net JAV vyriausybė priskyrė juo koduoti informaciją apie šalies karinę techniką.

Galime išskirti tokius bendrus reikalavimus:

- Būtina apsauga nuo išorinių įsilaužėlių firewall (“ugnies siena”)
- Kliento registracijos bei prisijungimo metu unikalaus saugos kodo įvedimas
- Būtinas duomenų kopijų kūrimas
- Būtina kiekvieno kliento autentifikacija
- Reikalinga nuolatinė antivirusinė priežiūra
- Kiti vartotojai, kurie nėra registruoti portalo duomenų bazėje, nukreipiami į prisijungimo (angl. login) puslapį

5.7. Kiti nefunkciniai sistemos parametrai

- Talpinamos informacijos išplėtimo reikalavimai – galimybė prisijungti naujiems klientams ir patalpinti savus IP adresus bei kitą informaciją
- Taikomųjų programų suderinamumas – suderinamumas su Microsoft programine įranga
- Reikalavimai servisui – kas tam tikrą laiko tarpą turi būti atliekamas sistemos saugumo ir stabilumo patikrinimas
- Resursų panaudojimas – pagrindinės duomenų apdorojimo operacijos vyks kompiuteryje, kur saugoma duomenų bazė, todėl bus apribotas galimų prisijungti prie duomenų bazės klientų skaičius iki 30 vienu metu (kai kuriems sistemos vartotojams bus galima prisijungti visą laiką).
- Turi būti naudojama tik licenzijuota programinė įranga.
- Programa turi nepažeisti Lietuvos Respublikoje galiojančių įstatymų bei teisės normų.
- Visos teisės į produktą priklauso užsakovui

6. Interneto serverių apsaugos testavimo sistemos testavimas

6.1. Naudojami testavimo tipai

Sistemų testavimas skirstomas kelias etapus:

- funkcinį testavimą,
- vartotojo sąsajos testavimą
- elementų testavimą.

Funkcinis testavimas tai toks, kai testuojama kaip sistema atlieka įvairias operacijas ir tikrinamas rezultatų teisingumas. Visos operacijos, kurias gali inicijuoti vartotojas, susiveda į darbo su duomenų baze operacijas (įterpimas, keitimasis, šalinimas). Tačiau atliekant funkcinį testavimą gilesnės tokio pobūdžio klaidos gali būti ir nepastebėtos – jos turi būti surastos kitais testavimo metodais. Taigi testavimo metu reikia stebėti tokias operacijų vykdymo dalis (vėliau klaidas galima detalizuoti kitais testavimo ir derinimo būdais):

1. duomenų pateikimas, siuntimas naudojant interneto naršyklę ir formas;
2. duomenų kontrolė (sintaksinė – neteisingos laukų reikšmės ir semantinė – duomenų bazės lygio);
3. papildomų užklausų generavimas (patvirtinimo, rezultatų atvaizdavimo puslapių);
4. operacijų ir kitų funkcijų atlikimas;
5. sekančio puslapio išdavimas.

Vartotojo sąsajos testavimas, tikrinant duomenų pateikimo teisingumą ir navigavimo kelius. Šis testavimo metodas skirtas aptikti sąsajos netikslumus, tokiu kaip klaidingi duomenų išvedimo formatai, įvedimo laukų apribojimai. Taip pat testuojant sąsają galima aptikti ir funkcionalumo klaidų, kurias detalizuojame atlikdami papildomą funkcinį testavimą ir vėliau – atitinkamų elementų testavimą.

Elementų (modulių) testavimas atliekamas realizavimo metu. Šis testavimo metodas pagrinde bus naudojamas realizavimo metu. Netgi neįtraukiant modulių į visą sistemą, o naudojant arba pagalbinius puslapius, arba tiesiogiai per interpretatorių (šiuo atveju PHP). Taip pat šis metodas leis lokalizuoti funkciniame ar sąsajos testavime aptiktas klaidas.

Į pirmuosius du testavimo metodus įtraukti ir vartotojai, pateikus jiems pirmines sistemos versijas. Tokiu būdu galime aptinkame klaidas, kurios nebuvo aptiktos pvz., dėl sistemos testuotojų ir projektuotojų kryptingo mąstymo. Tuo tarpu eilinis vartotojas gali aptikti pačias netikėčiausias klaidas, nes gali naudoti sistemą nenumatytais būdais.

6.2. Funkcinio testavimo ir sąsajos testavimo žingsniai

6.2.1. Nuorodų testavimas

Šiuo testavimo žingsniu atliekamas tokių funkcijų patikrinimas:

Ar teisingos nuorodos bei jų parametrai kiekviename funkciniame mygtuke?

Ar teisingos nuorodos bei jų parametrai vartotojui pateikiamuose puslapiuose?

6.2.2. Duomenų apdorojimo testavimas

Toliau einama duomenų apdorojimo testavimo, įvertinant tokius faktorius:

Ar įsijungia atitinkama tema, ją parinkus iš meniu?

Ar teisingai atpažįstama vartotojo darbo sesija?

Ar nepatenkama į pašalinius katalogus įvedus netinkamą nuorodą?

Ar informacija pateikiama iš naujai papildytų duomenų?

Ar informacija būtent tokia, kurios reikia konkretiems poreikiams?

Ar teisingai reaguojama į vartotojo nestandartiniu būdu suformuotus įėjimo duomenis?

Ar keičiant (redaguojant) informaciją pakeitimai išsaugomi tokie, kokie yra matomi ekrane?

6.2.3. Bendras valdymo testavimas

Testuojamas tokių funkcijų atlikimo korektiškumas?

Ar teisingai veikia vartotojo režimas?

Ar sėkmingai pateikiama pagalbinė informacija?

Ar visi elementai atlieka savo pasirinkimo funkcijas?

Ar teisingai apdorojamas operacijos patvirtinimo atšaukimas, koregavimas?

Ar teisingi įspėjančių ir klaidų pranešimų tekstai?

6.2.4. Pagalbos vartotojui sistema

Patikrinama ar pagalbos vartotojui sistema atitinka kontekstą ir jai keliamus tikslus.

6.3. Testavimo organizavimas

Ši programų sistema projektuojama – realizuojama modulinio prototipo principu. T. y. sukuriamas bazinis sistemos modulis, kuris pritaikomas papildomo funkcionalumo modulių integracijai. Pradžioje šalia bazinio modulio įdiegiami minimalaus funkcionalumo prototipiniai specializuoti moduliai, kurie vėliau išbaigiami iki specifikacijoje apibrėžto funkcionalumo.

Toks projektavimo – realizavimo modelis leidžia efektyvų sistemos testavimą, kadangi realizuojant vieną modulį, praktiškai naudojamasi kito modulio pateikiamu funkcionalumu, tuo pačiu jį testuojant. Hierarchinė programos struktūra neišvengiamai priveda prie hierarchiškai žemesnių dalių testavimo, kuriant hierarchiškai aukštesnes funkcionalumo dalis.

Galutinis testavimas atliekamas peržiūrint visus sistemos puslapius, sąsajas ir navigavimą tarp jų esant įvairioms, duomenimis apibrėžtomis, situacijomis. Taip pat buvo naudojamas funkcinio testavimo ir sąsajos testavimo planas (pagal 6.2. skyriaus funkcinio testavimo ir sąsajos testavimo žingsnius).

Dar vienas testavimo šaltinis – kolegos bei bendradarbiai, tiriantys šios sistemos naudą, universalumą bei vartojimo patogumą. Aptiktos klaidos, funkcionalumo, puslapio dizaino patobulinimų pasiūlymai bei pastabos buvo atitinkamai įvertinti ir pagal tai svetainėje padaryti atitinkami pakeitimai.

7. Išvados

1. Nors ir su tam tikru analitikų bei rinkotyrininkų skepticizmu, internetinės apsaugos testavimo sistemos atranda vietos bendruose verslo procesuose. Pagrindinė lėto jų plitimo problema yra ta, kad stokojama tokių pilnai integruotų internetinių-analitinių, o tuo pačiu ir teikiančių vartotojui informacines paslaugas, pagalbą, internetinių sistemų bei pačių projektų, kuriuose tai būtų galima integruoti.

2. Analitinėje darbo dalyje buvo išanalizuoti interneto serverių apsaugos programų testavimo sistemų ypatumai bei parenkama kūrimo metodika. Gilinamasi į pačią probleminę sritį ir galimus jos sprendimo būdus

3. Projektinėje darbo dalyje suformuojami pagrindiniai reikalavimai apsaugos programų testavimo sistemų veikimo modeliui, tokie kaip reikalavimai funkcionavimui, vartotojo sąsajai, eksploatavimo aplinkai, duomenų srautams. Pagal suformuotus kriterijus, sudaromas apsaugos testavimo sistemos modelis ir pritaikomas konkrečiai situacijai įgyvendinti.

4. Sistemos kūrimo ir jos testavimo stadijoje, naudojant PHP programavimo kalbą bei MySQL duomenų bazių valdymo sistemą, sukuriamas pats projektas ir vėliau integruojamas į internetinę svetainę. Atsižvelgiant į sistemos testuotojų pastabas ir pasiūlymus, padaryti atitinkami pakeitimai.

5. Apibendrinant projektuojamos internetinių serverių apsaugos programų testavimo svetainę ir pačios sistemos darbo eigą galima teigti, kad programinis produktas, kurio pagalba būtų galima supaprastinti ir pagreitinti silpnų vietų serverių apsaugos procesuose paieškas bei sprendimų siūlymą, atitinka jam iškeltus pradinius reikalavimus bei tikslus.

8. Terminų ir santrumpų žodynas

Vartotojas – bet kokios sistemos vartotojas, neturintis galimybių keisti sistemos konfigūraciją ir informaciją.

Administratorius – bet kokios sistemos vartotojas, turintis visas teises keisti sistemos konfigūraciją ir informaciją.

Internetas – pasaulinis kompiuterių tinklas.

WWW (*World Wide Web*) – viena iš interneto paslaugų – pasaulinė hipertekstinių dokumentų valdymo sistema.

Interneto naršyklė – programa, skirta peržiūrinėti interneto tiekiamus hipertekstinius dokumentus.

Interneto svetainė – hipertekstinių puslapių visuma, susijusi bendru kontekstu, informacija ir pan..

Interneto puslapis – tam tikro formato hipertekstinis dokumentas.

OS – operacinė sistema.

DB – duomenų bazė.

MySQL – duomenų bazių valdymo programavimo kalba.

HTTP – protokolas, skirtas perduoti duomenis internete.

HTML – hipertekstinių dokumentų tipas plačiai naudojamas internete.

PGP *(Pretty Good Privacy)* - kodavimo sistema, užtikrinanti duomenų konfidencialumą.

CRM (*Customer Relationship Management*) - kliento ryšių valdymo funkcijų tinkle pateikimas.

DFD (*Data Flow Diagrams*) – duomenų srautų diagramos parodančios detalesnę sistemos struktūrą.

FAQ (*Frequently Asked Questions*) - dažniausiai užduodami klausimai (liet. DUK).

UML (*Unified Modeling Language*) - modeliavimo kalba, naudojama objektiškai orientuotame projektavime.

9. Literatūra

1. McClure S., Shah S., Shah S. Web Hacking: Attacks and Defence. Addision-Wesley. 2003.- 374 p.
2. Black U. Internet Security Protocols. Prentice Hall PTR. 2000. - 279 p.
3. Kabir M. Apache Server 2 Bible. Dialektika Computer Publishing. 2001. - 672 p.
4. Allen J., Hornberger C. PHP 4 vadovas. Smaltija. 2003. 708 p.
5. Security Definitions [interaktyvus], 2004 [žiūrėta 2004-02-05]. Prieiga per internetą: https://fortress.wa.gov/dop/inetapp/DOP/Security.htm.
6. Как работает сканер безопасности? [interaktyvus], 2004 [žiūrėta 2004-02-05]. Prieiga per internetą: http://www.citforum.ru/internet/securities/scaner.shtml.
7. Security Metrics [interaktyvus], 2004 [žiūrėta 2004-04-23]. Prieiga per internetą: http://www.securitymetrics.com .
8. AuditMyPc [interaktyvus], 2004 [žiūrėta 2004-04-23]. Prieiga per internetą: http://www.auditmypc.com .
9. Shields UP!! [interaktyvus], 2004 [žiūrėta 2004-04-23]. Prieiga per internetą: http://grc.com.
10. Benjamin W. Web design pitfalls - Why website designs fail [interatyvus], 2004 [žiūrėta 2004-02-05]. Prieiga per internetą: http://www.ionix.com.au/articles/pitfalls.pdf.
11. Venčkauskas A. Informacinė sauga [ineraktyvus], 2002 [žiūrėta 2004-02-05]. Prieiga per internetą: http://www.ifko.ktu.lt/~algvenck/InfSauga/INF_SAUGkonspektas.pdf.
12. Безопасность WWW-серверов [interaktyvus], 2004 [žiūrėta 2004-02-05]. Prieiga per internetą: http://www.citforum.ru/internet/securities/wwwsec.shtml.
13. HTTPS and Webmin [interaktyvus], 2004 [žiūrėta 2004-02-05]. Prieiga per internetą: http://www.mandrakeuser.org/docs/secure/shttps.html.
14. Privacy International [interaktyvus], 2004 [žiūrėta 2004-02-05]. Prieiga per internetą: http://www.privacyinternational.org/
15. NetSec2004 [interaktyvus], 2004 [žiūrėta 2004-02-05]. Prieiga per internetą: http://www.gocsi.com/.
16. Central Intelligence Agency [interaktyvus], 2004 [žiūrėta 2004-02-05]. Prieiga per internetą: http://www.odci.gov/cia.