KAUNO TECHNOLOGIJOS UNIVERSITETAS
INFORMATIKOS FAKULTETAS
KOMPIUTERIŲ KATEDRA

Andrius Miškelevičius

Bankinių apmokėjimų pranešimų perdavimo sauga

Bank transfer payments messaging security

Magistro darbas

Vadovas: lekt. Dr. Dangis Rimkus
2010….m. ……mėn. ….d.

KAUNAS, 2010

KAUNO TECHNOLOGIJOS UNIVERSITETAS
INFORMATIKOS FAKULTETAS
KOMPIUTERIŲ KATEDRA

Andrius Miškelevičius

Bankinių apmokėjimų pranešimų perdavimo sauga

Magistro darbas

Recenzentas
Doc. dr. Gediminas Činčikas

2010-05-___

Vadovas
Doc.dr. Dangis Rimkus

2010-05-____

Atliko
IFN 8-3 gr. stud.
Andrius Miškelevičius
2010-05-15

Kaunas, 2010

TURINYS

SUMMARY

Nowadays, many banking payments takes place in cyberspace. Timeliness and convenience through several decades integrated banking systems in the business world. However e.commerce popularity integrated electronic banking systems into Web applications that are available to all users of electronic space. Payments in cyberspace creates significant added value to the economy as a whole but on a large spread banking systems increase sensitive security threat. The hostile actions in e.space damage per year increase to 1 trillion dollars, for the losses incurred by major reduction in investment in new technologies it resulting in further decrease in the level of safety. All IT professionals can help create a safer online space, because the future of electronic payments become more closely associated with our business and life.

The purpose of this work is to analyze banking systems safety and threats. In this work I designed and tested several banking systems and choose the best security solutions, to reduce security threats of electronic payments .

1 Įvadas

Šiais laikais daugelis bankinių atsiskaitymų vyksta elektroninėje erdvėje. Operatyvumas bei patogumas per kelis dešimtmečius bankines sistemas integravo į viso pasaulio verslą. Vis populiarėjant e. komercijai elektroninės bankininkystės sistemos integravosi į WEB aplikacijas, kuriomis gali naudotis visi elektroninės erdvės vartotojai. Atsiskaitymai elektroninėje erdvėje sukuria didelę pridėtinę vertę visai ekonomikai tačiau dėl didelio panaudojimo masto išaugo ir opios saugumo grėsmės. Dėl piktavališkų veiksmų el.erdvėje per metus padaroma žala siekia 1 trilijoną dolerių, dėl šių patiriamų didelių nuostolių mažėja investicijos į naujų technologijų diegimą ko pasėkoje dar labiau sumažėja saugos lygis.

Bankinių apmokėjimų programinė įranga, kuri apdoroja bankinius atsiskaitymus yra laikoma atskira sistemos dalimi, į kurią ji yra integruota. Ši posistemė lanksčiai ir paprastai integruojasi į bendrą sistemą ir efektyviai atlieka svarbias funkcijas susijusias su apmokėjimų apdorojimu. Bankinių apmokėjimų sistema skirta, operatyviai bei lanksčiai apdoroti mokėjimus bei apie įvykusius apmokėjimus informuoti tiek siuntėją, tiek ir gavėją.

2 Bankinių apmokėjimų pranešimų saugumo analizė

2.1 Tikslas

Pagrindinis šio darbo tikslas išnagrinėti ir išsiaiškinti bankinių apmokėjimų pranešimų sistemų saugumo spragas. Pasirinkti vieną bankinių apmokėjimų pranešimų sistemą. Detaliai išnagrinėti sistemos saugos spragas bei jas pašalinti. Išanalizuoti pavyzdinės sistemos saugumą prieš ir po saugos priemonių įdiegimo.

2.2 Uždaviniai

- Išanalizuoti silpnas bankinių apmokėjimų sistemų vietas
- Nustatyti potencialias grėsmes kiekvienoje sistemos dalyje
- Parinkti labiausiai tinkamą sprendimą kiekvienai saugumo grėsmei

- Suprojektuoti bei įgyvendinti vienos bankinės apmokėjimų sistemos saugą.
- Sumodeliuoti saugos priemonės atsparumą atakoms.

2.3 Nagrinėjama problema

Bankinių apmokėjimų sistemų įvairumas suteikia lankstumą bei tinkamą produkto pasirinkimą kiekvienam ūkio subjektui. Kiekviena bankinių apmokėjimų sistema remiasi saugumo technologija, kuri apsaugo sistemą nuo nesankcionuoto jos naudojimo. El. komercijoje naudojamos bankinės apmokėjimų sistemos remiasi keliais saugumo metodais, kurie nėra visiškai saugūs. Sistemos saugumo spragos gali įtakoti nesėkmingą jos naudojimą, ko pasėkoje gali susidaryti dideli finansiniai nuostoliai.

2.4 Mokslinio tyrimo tikslas ir uždaviniai

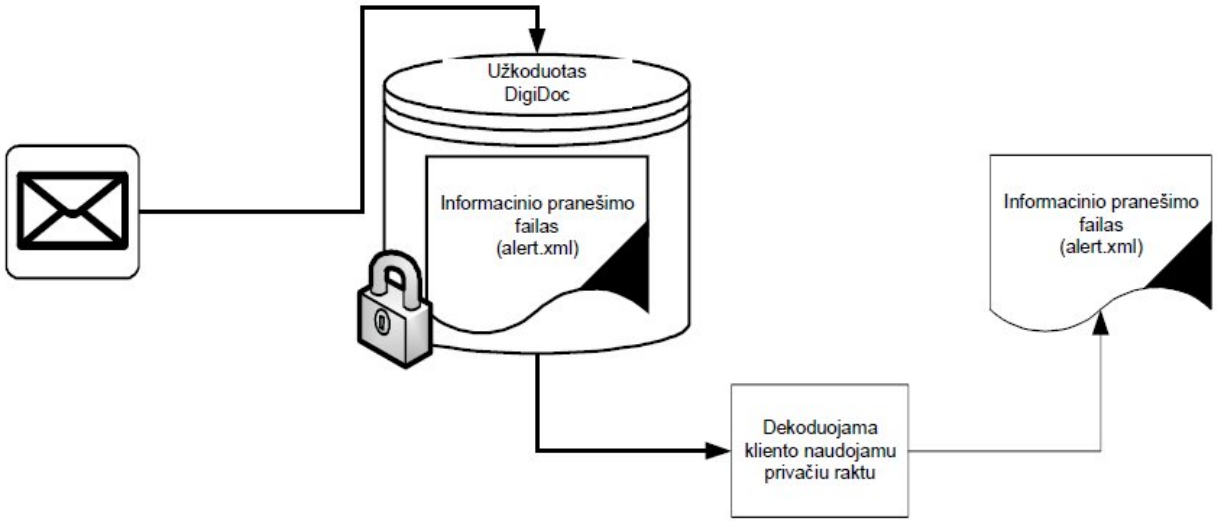
Tyrimo tikslas išsiaiškinti kaip saugiai perduoti duomenis bankinių apmokėjimų pranešimų sistemai bei apdorojus duomenis saugiai juos patvirtinti. Išsiaiškinti koki taikomi saugumo standartai. Tyrimu siekiama išsiaiškinti kokios techninės bei programinės priemonės padėtų užtikrinti saugų duomenų perdavimą. Taip pat svarbu nustatyti galimas aparatinės programos silpnąsias vietas.

Magistriniame darbe nagrinėjamos bankinių apmokėjimų pranešimų perdavimo saugos sistemų pažeidžiamumai, atsiradę dėl naudojamos technologijos trūkumų. Pateikiama sistemų struktūros analizė, išryškinami trūkumai ir privalumai bei trūkumų pašalinimo būdai. Darbo objektas yra bankinių apmokėjimų duomenų perdavimo sistemos. Tiriama kiekvienoje iš jų panaudotų saugumo elementų privalumai ir trūkumai. Pateikiama rekomendacija, kurią sistemą geriausiai naudoti konkrečiam projektui.

2.5 “Swedbank Gateway” sistemos analizė

Sweadbank vienas iš lyderiaujančių bankų Lietuvoje, turintis išvystytą bei patikimai veikiančią bankininkystės sistema, to pasėkoje el. prekybos sistemos naudoja Sweadbank bankines atsiskaitymų sistemas.

Swedbank Gateway“ – tai elektroninės bankininkystės sistema skirta visapusiškai valdyti savo bankines operacijas. Naudojimasis „Swedbank Gateway“ suteikia galimybę vykdyti didelius operacijų kiekius ir operatyviai gauti informaciją apie įvykusias bankines operacijas. Klientas integruoja „Swedbank Gateway“ paslaugą į savo turimą informacinę sistemą pagal banko nustatytus reikalavimus. Paslauga yra nesudėtingai integruojama į naudojamą įmonės finansinės apskaitos sistemą. Tai leidžia turėti realiame laike veikiančią automatizuotą sistemą kasdieninėms bankinėms operacijoms stebėti. Sistema siunčia informacinius pranešimus po kiekvienos bankinės operacijos įvykdymo. Bankinės apmokėjimų sistemos siunčiamas pranešimas yra koduotas XML tipo failas.[26]



1. pav. Informacinių pranešimų atsakymo gavimas iš banko

“Swedbank Gateway” sistemos privalumai:

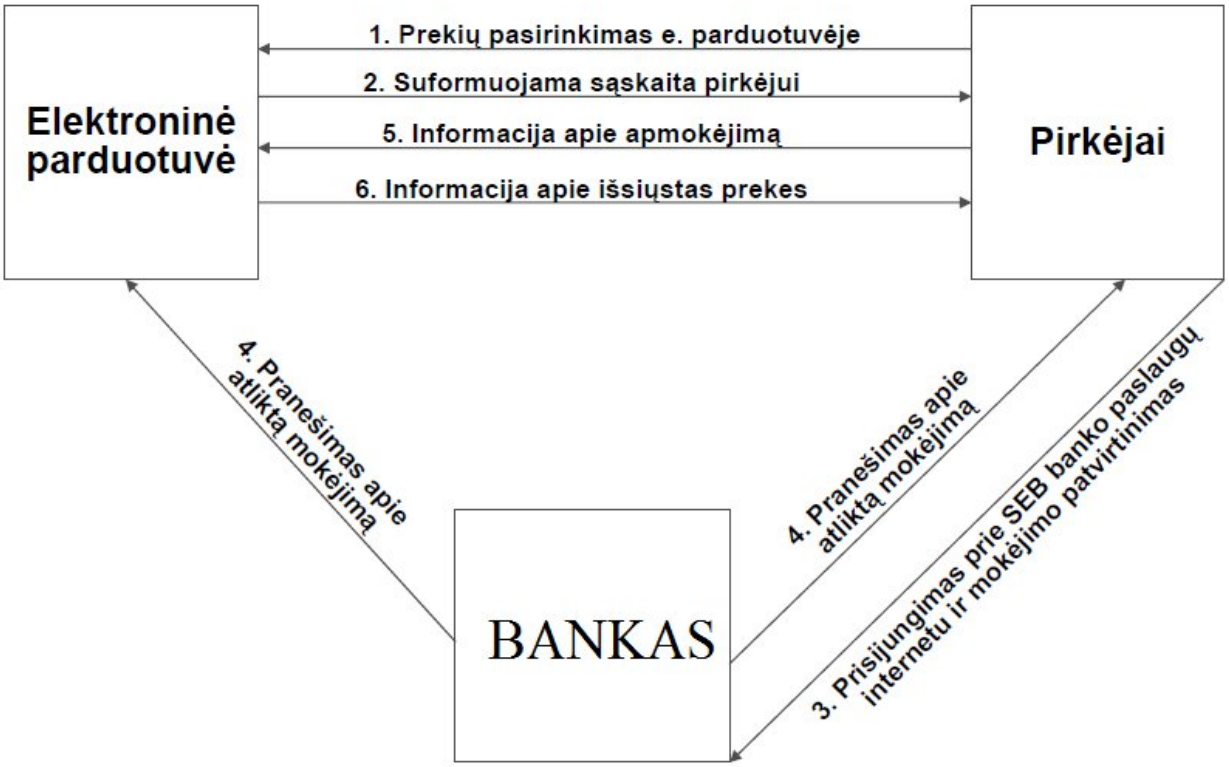
- Sistema yra lanksti ir lengvai integruojama į kitas informacines ūkio subjektų sistemas.
- Sistemos informaciniams pranešimams gauti nėra būtina siųsti užklausą dėl informacijos pateikimo, todėl išvengiama nesankcionuotų užklausų pateikimo. Sistemos pranešimai išsiunčiami po kiekvieno gauto apmokėjimo.

“Swedbank Gateway” sistemos trūkumai:

- “Swedbank Gateway” informaciniai pranešimai perduodami XML formato failuose, koduoti PKI technologijos pagalba, kuri nėra visapusiškai saugi dėl naudojamų algoritmų saugumo spragų.
- Reikalinga papildoma programinė įranga DigiDoc, gaunamų pranešimų dekodavimui. Būtina prieigos kontrolė prie DigiDoc programinės įrangos.
- Būtina turėti: ryšio sertifikatą bei kliento naudojamą privatų raktą;
- Dideli sistemos aptarnavimo kaštai:
    - Sutarties su banku pasirašymo mokestis 200 Lt.
    - Sistemos įdiegimo kaštai ~1000 Lt. (UAB „Online Media“, UAB "Informacinių technologijų organizacija" 850 Lt)
    - „Swedbank Gateway” palaikymo mėnesinis mokestis 130 Lt.
    - Informacinio pranešimo išsiuntimo „Swedbank Gateway” kanalu mokestis0.33 Lt.

2.6 “SEB Bank link” sistemos analizė

AB SEB bankas yra vienas iš didžiausių bankų Lietuvoje todėl daugelis el.bankininkystės sandorių sudaromi būtent per šio banko sistemą. AB SEB banko bankinių atsiskaitymų pranešimų sistema yra visiškai susieta su mokėjimais, todėl sistemos pranešimai apie apmokėjimus yra gaunami tik tuo atveju jeigu jie buvo atlikti per SEB Bank link sistemą. Duomenys, perduodami iš banko ir atvirkščiai yra elektroniniu būdu pasirašyti, tai leidžia patikrinti pateiktų duomenų teisingumą. Užklausos apie bankinius atsiskaitymus siunčiamos bei gaunamos HTTP GET arba HTTP POST komandų pagalba su nustatytais parametrais.[27]



2.pav SEB banko bankinių apmokėjimų sistemos veikimo schema

.

“SEB Bank link” bankinių apmokėjimų sistemos privalumai:

- Automatizuotas pirkimas –mažiau klaidų, palengvinama apskaita ir kontrolė

- E. parduotuvė gali nustatyti atsiskaitymo terminą, kad būtų išvengta atvejų, kai pirkėjas atsiskaito už baigusį galioti užsakymą
- Bankinių apmokėjimų pranešimas gaunamas tik su konkrečia el.prekybos sistema susijusiais apmokėjimais taip išvengiama papildomų el. sistemos duomenų bazės tikrinimo užklausų.

“SEB Bank link” bankinių apmokėjimų sistemos trūkumai:

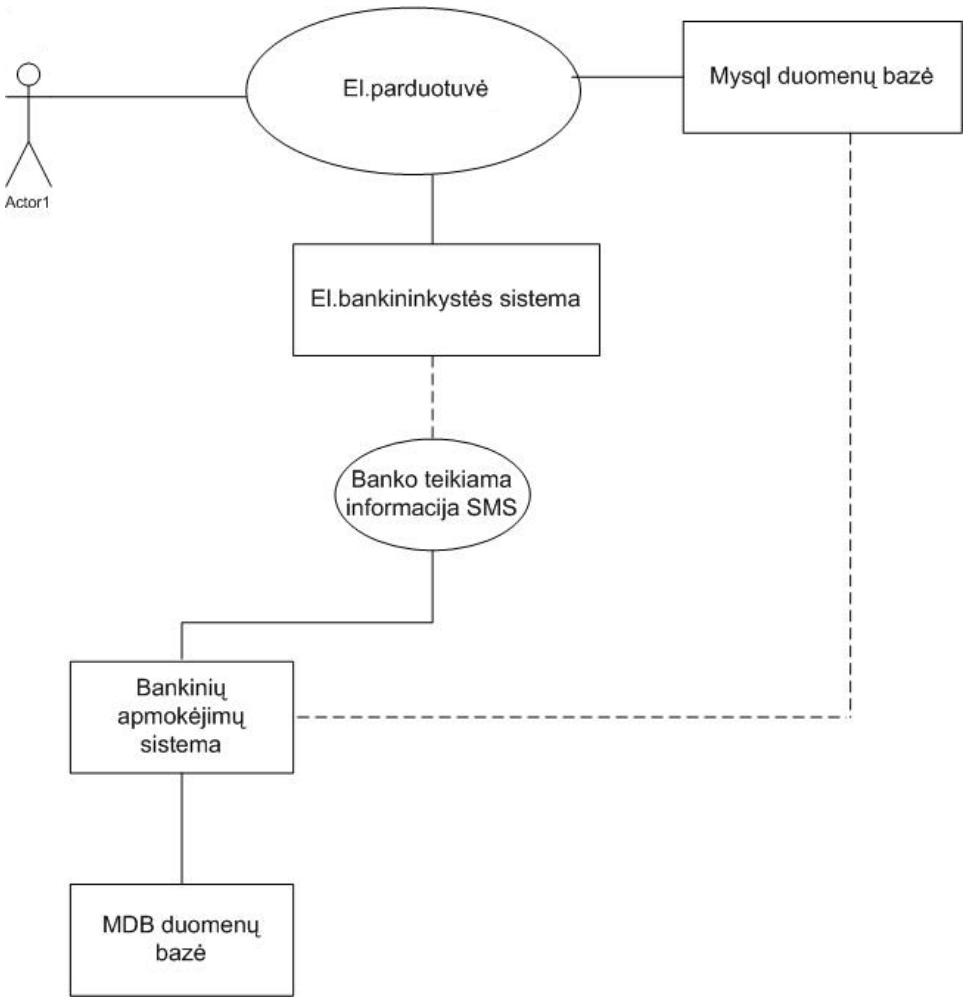
- Dėl skaitmeninio parašo pasirašymo autentifikacijos SEB bankinėje sistemoje nestabilumo, pasitaiko sistemos sutrikimo atvejų;
- Saugos spragos dėl naudojamo el. parašo technologijos SHA-1 saugos problemų.

- Dideli sistemos aptarnavimo kaštai:
    - Sutarties su banku pasirašymo mokestis 300 Lt.
    - Sistemos įdiegimo kaštai ~1000 Lt. (UAB „Online Media“ kaina 1130 Lt, UAB "Informacinių technologijų organizacija" 850 Lt)
    - Palaikymo mėnesinis mokestis 100 Lt.
    - Mokamas mokestis nuo kiekvieno užsakymo ~3%

2.7 „Free e-pay“ bankinių apmokėjimų pranešimų sistemos analizė

Sistema skirta mažiems elektroninės komercijos projektams. Bankinių apmokėjimų sistema „Free e-pay“ buvo sukurta minimaliai atsižvelgiant į saugos reikalavimus, nes ši sistema buvo naudojama apdoroti tik mažos vertės apmokėjimus tuo atveju, kai lėšų gavimo kaštai yra tampriai susiją su prekės marža.

Šios sistemos veikimo principas paremtas bankinės sąskaitos stebėjimu SMS pranešimais. Bankas gavęs apmokėjimą į kliento atsiskaitomąją sąskaitą išsiunčia apmokėjimą patvirtinančią trumpąją žinutę, kuri yra iš GSM aparato perduodama į „Bankinių apmokėjimų sistemą“. SMS žinutė analizuojama pagal identifikacinius laukus, jeigu visi tikrinami duomenų laukai atitinka užsakymo duomenis, užsakymas žymimas kaip korektiškas ir faktas fiksuojamas el.prekybos duomenų bazėje. Bankinių apmokėjimų sistemą sudaro dviejų tipų duomenų bazės. Lokali duomenų bazė, kurioje saugoma informacija apie gautas SMS bei išorinė naudojama užsakymo patvirtinimui.



3 pav. Bankinių apmokėjimų sistemos principinė schema.

Techniniai sistemos reikalavimai:

- Windows šeimos operacinė sistema (Windows 2000, Windows XP).
- Kompiuteris (serveris) su 500 Mhz spartos procesoriumi, 64 MB RAM atminties ir 10 MB laisvos vietos kompiuterio kietajame diske.
- Nuolatinis interneto ryšys ir nepertraukiamas elektros energijos tiekimas.
- Sistemoje privalo būti įdiegtas Microsoft .NET Framework 2.0 paketas
- GSM telefonas su Bluetooth technologija.

Sistemos saugumo trūkumai:

1 Banko siunčiama SMS gali būti perimta, suklastojus SIM kortelę.
2 Telefonas sujungtas su kompiuteriu per "Bluetooth" jungtį, todėl perduodami duomenys gali būti perimti su specialia programine įranga.
3 Programinė įranga patalpinta kompiuteryje, kuris prijungtas prie interneto ryšio, tai potenciali saugos spraga, nes kompiuteris gali būti apkrėstas virusais, trojanais ir kita kenkėjiška programine įranga.
4 Programinė įranga jungiasi prie nutolusios duomenų bazės ir siunčia nekoduotus duomenis apie apmokėjimą, šie duomenys gali būti lengvai perimti, modifikuoti arba suklastoti.
5 Tiesioginis įsilaužimas į tinklapį ar duomenų bazę,

„Free e-pay" sistemos privalumai:

- Maži sistemos aptarnavimo kaštai
- Sistema nereikalauja didelių techninių bei programinių parametrų.
- Paprastas integravimas į bet kokią el. prekybos sistemą
- Sistema nereikalauja jokių papildomo suderinamumo su banko sistemomis.
- Sistema gali turėti skirtingų teisių vartotojus.

„Free e-pay" sistemos trūkumai:

- Visos sistemos saugos trūkumai
- Apmokėjimų apdorojimo vėlavimas iki 4min. kritinio GSM tinklo apkrovimo metu.

2.8 Išvados

Išnagrinėjus keletą populiarių bankinių sistemų nustatyta, kad nepriklausomai nuo sistemos architektūros visos bankinės sistemos turi saugumo spragų. „Swead Bank Gateway“ bei „SEB bank link“ skirtos didesniems bei daugiau saugumo reikalaujantiems apmokėjimams apdoroti. Šios sistemos yra daug aptarnavimo sąnaudų reikalaujančios sistemos. „Free e-pay“ sistema yra pati nesaugiausia ir skirta mažoms el.prekybos sistemoms, kurios dėl mažų aptarnavimo kaštų pateisintų sistemos saugumo trūkumus.

2.9 Galimi atakų scenarijai

Kompiuteris pažeidžiamas DoS (denial of service) [22]- atkirtimo nuo paslaugos ataka. Atakos tikslas - paveikti kompiuterinę sistemą arba tinklą taip, kad kompiuterinės paslaugos taptų neprieinamos vartotojams. DoS atakos metu gali būti perkraunami kompiuteriniai resursai (perpildomas tinklas, apkraunama atmintis, CPU ir panašiai) arba sugadinama konfigūracija (pvz. maršrutizavimo informacija). Kompiuterinė sistema, stengdamasi apdoroti nereikalingą arba neteisingą informaciją sunaudoja daug savo resursų ir nebesugeba aptarnauti savo tikrųjų vartotojų. Galima modifikacija kai kompiuteris puolamas DDoS - tai paskirstyta DoS ataka, kai auką puola daug kompiuterių. Kadangi atakos šaltinių yra daug, apsisaugoti nuo tokios atakos yra itin sunku. Tokios atakos dažnai koordinuojamos naudojant botnet tinklą. Botnetas - virtualus kompiuterių tinklas, sudarytas iš interneto kirminais užkrėstų kompiuterių.[14]
Kompiuteris gali būti užkrėstas ne tik virusu bet ir kenkėjiška programine įranga vienas iš labiausiai paplitusių būdų perimti kompiuterio darbą apkrėsti jį trojanu. Trojanai nepanašūs į standartinius virusus ar kirminus, nes netrina tekstų ir nesisiuntinėja elektroniniu paštu. Trojanai kenkia žymiai skausmingiau- gali vogti bet kokią informaciją, įleisti įsilaužėlį į kompiuterį ir net duoti kažkam priėjimą ar visiškai kontroliuoti kompiuterį.

Viena iš galimų sunkiai suvaldomų grėsmių yra šnipinėjimo programinė įranga. Tai tokios programos, kurios, dažniausiai nežinant vartotojui, renka informaciją apie lankomus tinklalapius, vartotojo vardą, elektroninio pašto adresus, programas ar bylas, esančias kompiuteryje, arba registruoja vartotojo atliekamus veiksmus internete (pavyzdžiui, dirbant su banko sąskaitomis) ir siunčia šiuos duomenis tretiesiems asmenims (programų gamintojams ar

kitiems suinteresuotiems asmenims) be vartotojo leidimo ir netgi be jo žinios. Ši grėsmė yra pavojinga sistemai dėl galimybės perimti apmokėjimo informaciją.
Galimas informacijos perėmimas tinkle panaudojant įvairias priemones:

- Skenavimas - atvirų prievadų paieška, naudojama aktyvioms tinklinėms paslaugoms identifikuoti.
- Nesankcionuotas priėjimas prie sistemos vartotojo teisėmis.
- Nesankcionuotas priėjimas prie sistemos administratoriaus teisėmis.
- Tinklo paketų perėmimas, analizuojant jų turinį ir siekiant gauti slaptos informacijos, pavyzdžiui, vartotojų vardus, slaptažodžius ar pan.
- Pasitikėjimo eksploatavimas - apsimetimas kitu vartotoju ar kompiuteriu, siekiant gauti jam paskirtus resursus.[15]

Tinklo infrastruktūros atakavimas, siekiant sutrukdyti tinklo infrastruktūros darbą, pavyzdžiui, vardų serverių ir tinklo maršrutizatorių atakavimas.

2.10 GSM saugumo spragos

GSM ryšio saugumo spragos nepaisant pastoviai tobulinamo A5 algoritmo yra didelė problema. Šiuo metu Europoje naudojamas A5/1 algoritmas yra pažeidžiamas. Alex Biryukov, Adi Shamir and David Wagner įrodė kad šis algoritmas yra nesaugus ir yra pažeidžiamas. Naudodami vieną personalinį kompiuterį su 128 MB RAM ir dviem 73 GB kietaisiais diskais, sukūrė programą kuri palaužia algoritmą per pirmąsias 2 minutes, nuo duomenų siuntimo pradžios. Elad Barkhan, Eli Biham and Nathan Keller Izraelio Technikos universiteto studentai, įveikė algoritmą remdamiesi ciphertext-only pobūdžio ataka prieš A5/2 algoritmą kuris buvo palaužtas po kelių milisekundžių duomenų siuntimo. Šie asmenys taip pat aprašė atakų būdus ir kitiems GSM saugos algoritmams A5/1 bei A5/3. Šie pavyzdžiai parodo kad GSM ryšys nėra saugus ir būtina įdiegti papildomas saugumo priemones siunčiant duomenis tinkle.

2.11 Bluetooth saugumo spragos

Pagrindinis Bluetooth saugumo mechanizmas [4] – galimybė pasirinkti įtaiso veikimo režimą. Įvedus radimo (discoverable) režimą, įtaisą leidžiama „matyti“ kitiems, o slaptasis (non-discoverable) šią galimybę panaikina. Įtaisui dirbant radimo režimu, įsilaužėlis savo asmeniniu kompiuteriu gali nesunkiai atsisiųsti svetimus duomenis: adresų knygelę, darbotvarkę ir pan. Įjungus slaptąjį režimą, paieškos sistema įtaiso neranda ir jis į sąrašą neįtraukiamas, tačiau vartotojai, žinantys „paslėpto“ įtaiso MAC adresą, gali prie jo prisijungti. Taip gali nutikti įtaisams anksčiau užmezgus ryšio seansą (paired). Bluetooth adresus galima sužinoti dviem įtaisams besikeičiant duomenimis, net ir vartotojams įjungus duomenų šifravimo režimą. Tai įmanoma, nes dabartinis Bluetooth standartas nenumato MAC adreso šifravimo. Tiesa, dažnių keitimas (1600 kartų per sekundę) suteikia šiokią tokią apsaugą, tačiau keitimo dėsnis yra pseudoatsitiktinis. Teoriškai įsilaužėlis, naudodamasis tam tikra įranga, gali prisitaikyti prie vartotojų dažnių keitimo modelio. Kadangi šis modelis yra toks pats visame mini tinkle, piktadarys gali tuo bematant pasinaudoti. Jau dabar prekiaujama įranga, leidžiančia realiu laiku išanalizuoti perduodamus Bluetooth duomenų srautus. Tiesa, jos kaina dar labai didelė.
Gana dažnai žmonės patys perjungia savo mobiliuosius telefonus radimo režimu. Norint sujungti įtaisus tarpusavyje, bent vienas jų neturi būti slaptas. Be to, daugelis vartotojų šį režimą dažnai pamiršta išjungti ir tokiu būdu palengvina darbą įsilaužėliui. Šis bematant sužino telefono MAC adresą. Kadangi kiekvieno įtaiso adresas yra unikalus ir vartotojas jo keisti negali, įsilaužėliui pakanka jį sužinoti tik vieną kartą. Vėliau, net jei telefonas perjungtas slaptuoju režimu, piratas gali prie jo prisijungti. Aparato savininkas negali uždrausti to daryti ir net nepastebi užmegzto ryšio, nes šiuolaikiniai nešiojamieji įtaisai visada priima prašymą užmegzti ryšį L2CAP (Logical Link Control and Adaptation Layer Protocol) vartotojo apie tai neinformuodami. Jungiant įtaisus tarpusavyje (pairing), pastebima dar viena saugumo spraga. Prieš juos sujungiant, ekrane pateikiamas tik įtaiso vardas – jo adreso nematyti. Vardą gali pakeisti bet kuris vartotojas, todėl visiškai nesunku vienam įtaisui „apsimesti“ kitu. Jei egzistuoja Bluetooth interneto prieigos taškas, įsilaužėlis gali aktyvuoti savo įtaisą tuo pačiu vardu ir PIN kodu, kuris taip pat užtikrina interneto ryšį toje pačioje vietoje. Skirtumas tik tas, kad visa vartotojo asmeninė informacija (taip pat ir slaptažodžiai), siunčiama šiuo įtaisu, patenka į įsilaužėlio rankas.
Kitaip falsifikuoti vardą būtų galima per kai kuriose šalyse veikiančius Bluetooth „kioskus“, leidžiančius vartotojams už tam tikrą mokestį Bluetooth sąsaja atsisiųsti į savo telefonus žaidimus, melodijas, paveikslėlius ir pan. Priskyrę savo įtaisui „kiosko“ vardą ir PIN kodą,

įsilaužėliai gali į vartotojo mobilųjį įtaisą siųsti virusus ar kitas programas, padedančias lengviau pasiekti telefone esančią informaciją.

Taigi dėl netobulo standarto ir atsainaus gamintojų požiūrio į saugumą Bluetooth technologija nėra visiškai saugi. Tačiau nors egzistuoja nemažai būdų, kaip pasinaudoti Bluetooth saugumo spragomis, kai kurie asmenys gali pamanyti, jog ryšys veikia nedideliu atstumu, todėl dažnai galima vizualiai nustatyti įsilaužėlį. Kartais įsilaužėliai naudojasi kryptinėmis Bluetooth antenomis ir stiprintuvais, didinančiais Bluetooth veikimo spindulį iki kilometro. Todėl geriausia apsauga – atnaujinti telefono programinę įrangą ir jungti Bluetooth tik tada, kai to tikrai reikia.

“Bluetooth” atakų tipai:

BlueSnarf. Tai jungimasis prie kai kurių Bluetooth įtaisų modelių be jų savininko leidimo (t. y. įtaisas neprašo patvirtinti leidimo prisijungti ir net nerodo, kad perduodami duomenys). Tokiu būdu prisijungus galima pasiekti paprastai draudžiamas telefono atmintinės vietas: telefonų knygelę, kalendorių ir darbotvarkę, telefono IMEI (International Mobile Equipment Identity) numerį ir pan. Paprastai taip atakuojami radimo režimu veikiantys telefonai, tačiau, sužinojus MAC adresą tam skirtomis programomis (bluesniff, btscanner, redfang ir kt.), gali būti atakuojami ir slaptojo režimo telefonai.

Backdoor. Šios atakos esmė – pasibaigus normaliam ryšio seansui (pairing) Bluetooth sąsaja ir aukai ištrynus įsilaužėlio įtaisą iš sujungimų sąrašo (paired device list), ryšys tęsiamas, o įsilaužėlis gali naudotis vidiniais telefono ištekliais. Jis gali ne tik pradėti siųsti duomenis, bet ir prisijungti vidiniu aukos telefono modemu prie interneto, pasitelkęs WAP ar GPRS. Be to, jei ši ataka sėkminga, įmanoma ir Bluesnarf ataka, net jei ji anksčiau šio telefono nepaveikė. Apsisaugoti nuo Backdoor atakos galima tik visiškai ištrynus įtaisą iš sujungimų sąrašo, o tai padaryti pavyksta tik atkūrus telefono pradines nuostatas. Tačiau tai padarius, dingsta visa vartotojo asmeninė informacija.

BlueBug. Šios atakos metu Bluetooth sąsaja sukuriamas nuoseklusis ryšys tarp įsilaužėlio ir aukos įtaisų. Piratas gali naudotis telefono AT komandomis, taigi – visiškai kontroliuoti telefoną: prisijungti prie interneto ir perduoti duomenis, skaityti bei siųsti SMS, tvarkyti kontaktus, peradresuoti skambučius ar net skambinti pasirinktu numeriu. Vadinasi, jis gali perimti atkeliaujančius aukos skambučius ir nukreipti mokamais numeriais. Apsisaugoti nuo šios ir BlueSnarf atakų (bent jau kol kas) galima tik išjungus Bluetooth.

Bluejacking. Tai socialinė ataka. Jos tikslas – priversti vartotoją sujungti (pairing) savo telefoną su įsilaužėlio įtaisu. Bluejacking ataka vykdoma masinėse žmonių susibūrimo vietose, parinkus

žmones dominantį įtaiso vardą (Bluetooth standartas leidžia pasirinkti iki 248 simbolių įtaisų vardus). Tarkim, įsilaužėlis savo įtaisui parenka vardą PIN1234 ir pradeda jungtis su jam matomais vartotojų telefonais. Vartotojas, pastebėjęs tokį užrašą ekrane, gali surinkti PIN kodą 1234 ir patvirtinti ryšį tarp įtaisų, tokiu būdu užtikrindamas įsilaužėliui visišką savo telefono kontrolę. Bandymai žmonių susibūrimo vietose (konferencijose, technologijų parodose ar net didelėse parduotuvėse) parodė, kad į kvietimą užmegzti ryšį atsako vidutiniškai 3 iš 10 kvietimą gavusių žmonių.

Sistemos kompiuterio pažeidžiamumas

Kompiuteris su sistema prijungtas prie interneto ryšio, tačiau kompiuteris naudojamas tik vienam tikslui - sistemos aptarnavimui. Ši sistemos vieta yra viena iš labiausiai pažeidžiamų todėl jai apsaugoti būtina įdiegti visas būtinas apsaugas.

Sistemos grėsmių įvertinimas

Saugumo spraga	Pažeidžiamumo lygis	Reikalingos saugos priemonės
Įsilaužimas tiesiogiai į tinklalapį	aukštas	Programinės
SMS žinutės nuskaitymas „bluetooth“ ryšiu	žemas	Techninės
Informacijos perėmimas sistemos kompiuteryje	aukštas	Programinės
Informacijos perėmimas siunčiant nekoduotus duomenis tinklu	aukštas	Programinės
SMS žinutės nuskaitymas pasinaudojant A5/1 spragomis	žemas	Programinės

1 lentelė. Sistemos grėsmių įvertinimas

2.12 Populiariausių saugumo sistemų palyginimas duomenų apsaugai tinkle

Siunčiant informaciją tinkle būtina pasirūpinti, kad siunčiama informacija būtų apsaugota nuo nesankcionuoto jos panaudojimo. Saugumo lygis priklauso nuo naudojamos technologijos. Šiuo metu yra daug programinių priemonių galinčių siunčiamus duomenis apsaugoti nuo kenkėjiško jų panaudojimo.

Šiuo metu naudojami duomenų apsaugos metodai:

- **Kriptografinis šifravimas –** remiasi tam tikrais šifravimo algoritmais, kurie duomenis patikimai užšifruoja tam tikro ilgio tam tikra matematine funkcija.
    - **DES algoritmas** (Data Encryption Standard – duomenų šifravimo standartas) – blokinis simetrinis algoritmas, kurio blokų ilgis yra 64 bitai, rakto ilgis yra 56 bitai. DES duomenų šifravimo standartu paskelbtas JAV 1977 metais.
    - **AES algoritmas** (angl. Advanced Encryption Standard – pažangus šifravimo standartas) – šifravimo algoritmas, 2001 metais JAV paskelbtas standartu. Dar vadinamas Rijndael algoritmu, jo autoriai yra Joan Daemen ir Vincent Rijmen. Rijndael yra blokinis simetrinis algoritmas. Šifravimo raktai gali būti 128, 192, arba 256 bitų ilgio, o blokų ilgis gali būti 128, 192 arba 256 bitų.
      Etapo rakto sudarymas iš šifro rakto susideda iš dviejų pagrindinių dalių: rakto plėtimas ir etapo rakto pasirinkimas.
    - **RSA algoritmas -** RSA yra viešojo rakto tipo kriptosistema, kuri palaiko duomenų šifravimą ir skaitmeninius parašus. RSA nėra labai greitas algoritmas. DES iki 100 kartų greitesnis, tačiau ir silpnesnis už RSA. RSA laboratorija rekomenduoja naudoti 1024 bitų ilgio raktą. Labai svarbiems duomenis koduoti naudokite 2048 bitus.
    - **MD5 algoritmas** (Message-Digest algorithm 5) – žinutės santraukos algoritmas, plačiai naudojama kriptografijos maišos funkcija su 128 bitų (16 baitų) maišos reikšme. Labai populiarus algoritmas. Ima fiksuoto dydžio žinutę ir išveda 128 bitų "pirštų antspaudą". Naudojamas viešojo rakto kriptosistemose skaitmeniniams parašams daryti.
    - **SHA-1 algoritmas** (Secure Hash Algorithm) – dar vienas populiarus algoritmas, naudojamas įvairiose programose ir protokoluose kaip antai – TLS, SSL, PGP,

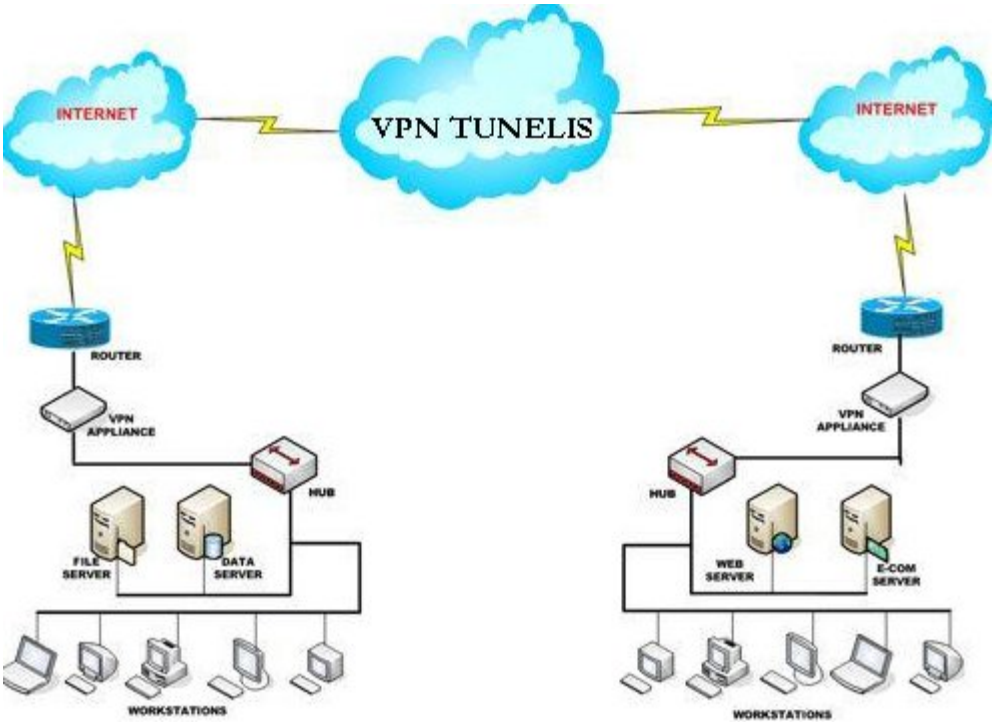
SSH, S/MIME, IPSec. SHA-1 buvo laikomas pažeidžiamo MD5 algoritmo įpėdiniu, tačiau 2004 ir 2005 metais atrasti pažeidžiamumai daro šį algoritmą nerekomenduotinu. Yra sukurta saugesnių SHA-1 algoritmo variacijų (SHA-224, SHA-256, SHA-384, SHA-512), kuriose pažeidžiamumų kol kas nerasta. SHA-1 apskaičiuoja 160 bitų parašą:[6]

- **PGP šifravimo algoritmas** PGP (Pretty Good Privacy) ─ vienas populiariausių ir stipriausių šifravimo algoritmų. PGP naudoja viešojo rakto kriptografiją. Prieš šifruodama duomenis PGP programa suspaudžia (suarchyvuoja) tekstą. Tai duoda nemažą pliusą saugumui: dauguma kriptoanalizių panaudoja iškarpų sutapimą duomenų dešifravimui. Archyvuojant tekstą jis šiek tiek iškraipomas, taip sumažinant galimybę sėkmingai panaudoti tokią ataką.

2.13 Patikimo metodo pasirinkimas

Visi naudojami šifravimo algoritmai turi savo trūkumų bei saugumo spragų, todėl naudojami atskirai nėra efektyvūs ir saugūs. Norint apsaugoti siunčiamus bankinių apmokėjimų pranešimų duomenis būtina naudoti patikimą metodą, kuris remtųsi keliomis šifravimo technologijomis vienu metu.

Vienas iš patikimiausių ir technologiškai pažengusių metodų yra VPN – virtualus privatus tinklas. VPN tuneliavimas naudoja viešąją tinklinę terpe persiusti duomenis tarp dviejų privačių tinklu. Duomenys ir kita informacija, kuri perduodama tuneliu, gali būti kitu protokolų dalys. Tunelio protokolas duomenų paketus paslepia po papildoma antrašte, skirtingai nei kiti protokolai, kurie siunčia viska atvira forma. Papildomoje antraštėje yra maršruto informacija, kad duomenys būtų perduodami tinklu tiksliai iki gavėjo. Informacijos paketai perduodami per tinklą nuo tunelio pradžios iki pabaigos. *Tunelis* – tai loginis kelias, kurio informacijos vienetai keliauja viešuoju tinklu. Kai informacijos paketai pasiekia tikslą, jie yra priimami, iškoduojami ir perduodami iki galutinio tikslo jau privačiame tinkle. Tuneliavimas aprėpia informacijos paketų suskaidymą (užkodavimą), siuntimą ir priėmimą (iškodavimą).[7]



4 pav. VPN veikimo grafinis vaizdavimas

VPN naudojami protokolai

IPSec – tai interneto Draft standartas (angl. Internet Draft Standard), kuris buvo sukurtas IETF (Engineering Task Force) darbo grupės, užtikrinantis saugų informacijos perdavimą per viešuosius IP tinklus.

IPSec [2] yra 3 lygio protokolo standartas, kuris sujungia kelias skirtingas apsaugos technologijas, užtikrinančias konfidencialumą, vientisumą ir autentiškumą. *IPSec* protokolas realizuoja tinklo lygio šifravimą ir autentifikacija, naudodamas end-to-end tinklinės architektūros technologija.

IPSec naudoja:

- Diffie-Hellman raktų apsikeitimo technologiją gauti rakta tarp dviejų taškų viešame tinkle.
- Viešojo rakto kriptografiją garantuojančią dviejų pusių privatumą ir išvengti tarpininkavimo (man-in-the-middle) atakų.
- Duomenų šifravimo standartą (DES), duomenų šifravimui.
- Duomenų kodavimo algoritmus MD5, SHA.
- Skaitmeninius parašus, sertifikatus, patvirtinančius autentiškumą ir naudojamas kaip skaitmeninės identifikavimo kortelės.

IPSec palaiko du šifravimo režimus: *transporto* ir *tunelio*. *Transporto* režimas šifruoja tik pačius duomenis kiekviename pakete, bet palieka protokolo antraštę nešifruotą. Daug saugesnis *tunelio* režimo šifravimas, nes ten užšifruojamas visas paketas – tiek duomenys, tiek antraštė. Gavėjo pusėje yra IPSec serveris, skirtas duomenų atkodavimui. Toks serveris turi būti tiek pas siuntėja, tiek pas gavėją, serveriai turi dalintis viešaisiais raktais (public keys). Tai įgyvendinama pasitelkus protokolą Internet Security Association and Key Management Protocol (ISAKMP), kuris leidžia gavėjui gauti viešąjį rakta ir autentifikuoti siuntėją pasinaudojant skaitmeniniu parašu.

PPTP(Point-to-Point Tunneling Protocol) – šio protokolo kūrėjai yra didieji gamintojai tokie kaip US Robotics, Ascend Communications, 3Com/Primary Access, ECI Telematics ir Microsoft. Tačiau dauguma vartotojų naudoja Microsoft protokolo versiją. PPTP – tai antro lygio protokolas ir yra sukurtas iš populiaraus Internetinio PPP (Point-to-Point Protocol) ir TCP/IP (Transmission Control Protocol/Internet Protocol) protokolų. PPP palaiko kelis protokolus, turintis duomenų autentifikacijos, privatumo ir suspaudimo metodus. PPTP specialiai buvo sukurtas kaip duomenų apjungimo (angl. encapsulation) mechanizmas, perduodanti duomenis tik ne TCP/IP (non-TCP/IP) protokolais, tokiais kaip IPX ir Appletalk, per Internetą naudojant GRE (Generic Routing Encapsulation) technologiją. Ši technologija skirta apsaugoti TCP/IP srautą tarp Windows 95/98/NT klientų, prisijungusių prie interneto per PPP ir Windows NT serverius, esančius vietiniame tinkle, už ugniasienės. PPTP naudoja TCP sujungimą tunelio palaikymui ir GRE, apjungti PPP kadrus (angl. frames) tunelio duomenims. Tuneliavimas realizuotas PPTP pagalba, nes šis protokolas apjungia paketus, įdėdamas paketo informaciją (IP, IPX, ar NetBEUI) į IP paketo vidų, perdavimui per internetą. Pasiekęs gavėją išorinis IP paketas yra „nuimamas“, paliekant originalų paketą. Apjungimas (angl. encapsulation) leidžia transportuoti paketą, kuris be apjungimo negalėtų saugiai būti perduotas per internetą.

L2TP (Layer 2 Tunneling Protocol) – Antro lygio tuneliavimo protokolas. Microsoft ir Cisco sujungę PPTP ir L2F protokolų geriausias savybes, taip buvo sukurtas tuneliavimo standarto protokolas pavadintas L2TP. L2TP yra tinklo protokolas palengvinantis PPP kadrų tuneliavimą per viešąjį tinklą. Jis apjungia PPP kadrus siuntimui per IP, X25, Frame Relay ar ATM tinklus. Apjungtų PPP kadrų duomenys užšifruojami ir/arba suspaudžiami. L2Tp gali būti naudojamas tiesiai per įvairius WAN tinklus. L2TP naudoja UDP ir serija L2TP žinučių, tunelių palaikymui IP tipo tinkluose. L2TP leidžia daugialypius tunelius per tą patį abipusį ryšį.

2.14 VPN privalumai:

- Saugus duomenų perdavimas, nes koduojami visi duomenys.
- Geografiškai išsibarsčiusių tinklų sujungimas;
- Galima lengvai ir greitai išplėsti esamą tinklą;
- Supaprastina tinklo valdymą ir pagerina jo kokybinius parametrus; [8]
- Nutolusiems tinklams, filialams, darbuotojams prisijungti prie įmonės tinklo resursų (programinių, techninių), ;
- Duomenys perduodami saugiu ir trumpiausiu keliu.
- Taupomos lėšos bei didėja darbo efektyvumas.[5]

2.15 VPN trūkumai:

- greitaveikos sumažėjimas dėl informacijos kodavimo
- neužtikrinamas pastovus duomenų srauto perdavimo greitis
- “end-point security” neužtikrina VPN tinklo saugumo dėl galimybės suklastoti, modifikuoti ar nuskaityti siunčiamus duomenis [1]
- kadangi duomenys tinkle keliauja koduoti, sunku apskaityti siunčiamų bei gaunamų duomenų kiekius.

VPN technologija nėra visapusiškai saugi, todėl būtinos papildomos priemonės užtikrinančios saugų VPN veikimą. Duomenų perdavimui iš bankinių apmokėjimų sistemos nutolusiai tinklapio duomenų bazei naudojama VPN technologija sukurti saugų tinklą tarp nutolusio kompiuterio bei serverio. Dėl VPN nepakankamo “end-point security” tikrinimo sistema nėra saugi, todėl virtualiame tinkle keliaujantys duomenys gali būti perimti. Šiai problemai išspręsti bus panaudojama SSH technologija kai VPN tinkle duomenys bus perduodami SSH pagalba, tokiu būdu perėmus duomenis jie nebus nuskaityti ir panaudoti.[9]

2.16 SSH panaudojimas

- Su SSH klientu, kuris palaiko terminalo protokolus (terminal protocols) galima nuotolinių būdu prisijungti prie serverio ir atlikti norimus nustatymus.
- Naudojamas kartu su FTP protokolu, ir taip gaunama saugi alternatyva SFTP.
- Kartu su rcp (atsarginės duomenų kopijos) ir gaunamę saugią atsarginių kopijų darymo alternatyvą SRCP (Secure Remote Copy).
- Taip pat ssh galime panaudoti prievadų atidarymui (port forwarding) arba tuneliavimui (tunneling) , tai galima panaudoti kaip alternatyvą VPN (Virtual private network). Tokiu atveju nesaugūs TCP/IP sujungimai yra peradresuojami į SSH ir SSH vykdo saugų duomenų perdavimą. Tokia technologiją naudojama jungiantis prie duomenų bazių, e-pašto serverių.
- SSH serveris, kuris palaiko dinaminį prievadų atidarymą, gali būti panaudotas kaip proxy serveris , saugiam naršymui internete.
- Per SSH klientą, kuris paliko exec sesijas, galimas tinklo įrenginių monitoringas.

Čia paminėta keletas pagrindinių ssh funkcijų, kurių yra daugybė ir visas jas išvardinti būtų sunku.

SSH saugumas

- man-in-the-middle ataka, tai problema su kuria susiduria SSH-1 vartotojai. Ši problema buvo beveik išspęsta su SSH-2 atsiradimu. Tačiau praktikoje kartais vis dar pasitaiko tokio tipo atakų.
- Visuose SSH versijose labai svarbu patikrinti nežinomus, naujus viešus raktus, nes patvirtinus tokį raktą kaip patikimą, kenkėjams darosi paprasčiau įvykdyti man in the middle ataką.
- Jei SSH versija turi visas pataisas, paslauga tariamai laikoma saugia, nes šifruoja tinklu perduodamus duomenis. Tačiau tai viena iš paslaugų, prieš kurią pastaraisiais metais dažnai nukreipiamos grubaus slaptažodžių (brute-force) laužimo atakos. Aktyviai įsilaužiama į sistemas su silpnais eilinių vartotojų SSH slaptažodžiais. Po to, padidinus privilegijas, būdavo gaunamos root teisės ir įdiegiamos rootkit priemonės įsilaužimui nuslėpti. Svarbu žinoti, kad pilnas slaptažodžių perrinkimas gali būti vienas iš metodų įsilaužti net ir į visas saugumo pataisas turinčią sistemą. Norint sutrukdyti tokias atakas,

rekomenduojama naudoti viešo rakto autentifikacijos metodą, kurį palaiko dauguma SSH realizacijų, pavyzdžiui OpenSSH. Tokios atakos gali būti naudojamos ir prieš kitas interaktyvias paslaugas.

2.17 SSH privalumai:

- Saugus duomenų perdavimas, nes koduojami visi duomenys.
- Paprastas konfigūravimas
- Greitas bei efektyvus būdas perduoti šifruotą informaciją tinkle.
- Taupomos lėšos bei didėja darbo efektyvumas.

2.18 SSH trūkumai:

- „Brute force“ atakų neatsparumas. [25]
- Prastas autentifikavimo mechanizmas

Kriterijai	**VPN**	**SSH**
Reikalavimai vartotojui	Technologija reikalauja pakankami daug IT žinių	Paprasta naudoti ir eiliniam vartotojui
Naudojamos saugumo technologijos	IPSec, SSL, L2TP	SSL – kriptografinis protokolas
Greitaveika	Sumažėjimas dėl informacijos šifravimo	Sumažėjimas dėl informacijos šifravimo
Sistemos saugumas	Nėra visiškai saugi.	Nėra visiškai saugi.
Aptarnavimo kaštai	Pakankamai dideli jeigu naudojama techninė įranga	Maži

2lentelė. Palyginamoji VPN bei SSH technologijų lentelė

Atlikus išsamią VPN bei SSH technologijų analizę, duomenys matomi 2 lentelėje. Matome, kad abi technologijos naudoja pakankamai daug saugumo priemonių tačiau nėra visiškai saugios. Dėl duomenų šifravimo greitaveika mažėja abiejų technologijų panaudojimo atveju. SSH technologija reikalauja šiek tiek mažiau IT žinių, be to aptarnavimo kaštai yra mažesni nei VPN. Bankinių apmokėjimų sistemos „Free e-pay“ saugai tarp dviejų nutolusių duomenų bazei užtikrinti bus naudojamas dvigubas tuneliavimas. Tarp nutolusių duomenų bazių sukuriamas VPN tunelis, kuriame vyksta susijungimas tarp duomenų bazių per SSH technologiją.

Duomenų autentifikacija

Ne mažiau svarbi duomenų apsauga yra autentifikavimas, kuris užkerta prieiga prie tinklo nepageidaujamiems asmenims ir leidžia prieigą legaliems vartotojams. Autentifikavimas gali būti vykdomas keliais būdais:

- autentifikuojamasis įrodo savo tapatybę pasakydamas slaptažodį ar bendrai žinoma informaciją
- autentifikuojamasis gali pademonstruoti, kad jis disponuoja kokiu unikaliu daiktu (fiziniu daiktu), kuriuo gali būti pvz. elektroninė magnetinė kortelė
- autentifikuojamasis gali būti atpažintas pagal pirštų antspaudą, akies rainelę ir kituos biometrinius duomenis iš anksto įtrauktus į autentifikatoriaus duomenų bazę

Autentifikavimo algoritmus butų galima suskirstyti į skirtingus metodus [24]:

- Paprastas slaptažodis
- Vienkartinis slaptažodis
- Užklausa – atsakymas
- Anonimiškas raktų apsikeitimas
- Slaptas slaptažodžio patvirtinimas

Paprastas slaptažodis tai pats paprasčiausias autentifikavimo metodas. Klientas pateikia vartotojo vardo ir slaptažodžio porą serveriui neapsaugotu kanalu (pvz.: TCP/IP protokolu). Tuomet serveris gavęs vartotojo vardą ir slaptažodį palygina juos su atitikmenimis savo duomenų

bazėje ir jei jie sutampa, vartotojas būna autentifikuotas ir gauna leidimą prisijungti prie sistemos. Jei serveryje vartotojų slaptažodžiai būtų laikomi neužšifruoti, piktavaliai galėtų įsilaužti į serverio duomenų bazę ir taip sužinoti visų vartotojų prisijungimo duomenis. Siekiant to išvengti, slapta informacija serveryje yra koduojama „hash“ algoritmu ir informacija tampa neprieinama trečiosioms šalims. Dėl to, serveris gavęs vartotojo slaptažodį jį turi konvertuoti jam vienam žinoma „hash“ funkcija ir taip duomenų bazėje surasti atitikmenį.

Vienkartinis slaptažodis, atrodytų, gali būti panaudotas tik vieną kartą. Šis metodas yra paprasto slaptažodžio patobulinimas, kuomet sistemoje reikia tik nežymių serverio patobulinimų. Vartotojas yra aprūpinamas slaptažodžių sąrašu, kur kiekvienas gali būti panaudotas tik kartą arba naudojamas procesorius ar netgi kortelė (SecureID), kurie generuoja slaptažodžius pagal numatytą algoritmą. Kadangi slaptažodžiai naudojami tik kartą, jie gali būti drąsiai siunčiami neapsaugotais kanalais. Autentifikavimo serveris saugo paskutinį gautą vartotojo slaptažodį P[i] ir tuo metu kai gauną sekantį slaptažodį P[i-1] iš to pačio vartotojo, naudodamas „hash“ algoritmą, perskaičiuoja naują reikšmę turėtos P[i] reikšmės ir palygina su gautąja. Jei reikšmės sutampa, serveris autentifikuoja vartotoją ir savo duomenų bazėje seną slaptažodį pakeičia naujuoju ir laukia kito prisijungimo.

Užklausos – atsakymo autentifikacijos metodas yra gana dažnai naudojamas praktikoje ir remiasi prielaida, jog vartotojas gali sugeneruoti atsakymą tinklui pasinaudodamas savo slaptažodžiu ar sudėtingesne paslaptimi. Užklausa paprastai būna atsitiktinai sugeneruota reikšmė, kuri negali kartotis. Užklausa yra persiunčiama vartotojui, pastarasis turi atsakyti užklausos ir bendro rakto funkcijos reikšme.

Visi trys prieš tai aptarti autentifikavimo metodai gali būti sustiprinti *anonimišku raktų apsikeitimo* metodu. Jei ryšio kanalas, kuriuo perduodami autentifikacijos duomenys yra užšifruotas ir apsaugotas nuo pranešimų turinio pakeitimo, tuomet toks metodas kaip „paprastas slaptažodis“ gali būti saugiai naudojamas. Tačiau diegiant minėtą saugų kanalą, šifravimo raktai kažkokiu būdų turi būti perduoti abiem ryšio seanso dalyvių pusėms. Mokslininkai Whitfield Diffie ir Martin Hellman pateikė sprendimą ir jį pavadino „Diffie-Hellman“ metodu. Šis metodas remiasi viešo rakto kriptografija ir leidžia ryšio seanso dalyviams, prieš tai nieko nežinojusiems vienam apie kitą, apsikeisti slaptais šifravimo raktais nesaugiu kanalu. Ryšio seanso pradžioje vartotojas ir serveris apsikeičia savo viešais raktais ir jais koduoja pranešimus, o atkoduoja savo privačiais raktais.

Slapto slaptažodžio patvirtinimo metodas autentifikavimo sistemose dažnai naudojamas tuomet, kai vienas ryšio seanso dalyvis siekia įrodyti savo autentiškumą antram seanso dalyviui, tačiau nenori, kad niekas (kartu ir antrasis ryšio seanso dalyvis) ką nors sužinotų apie naudojamą slaptažodį. Šio metodo dėka vietoj paprasto slaptažodžio nesaugiu kanalu siunčiamas dvejetainis skaičius. ZKPP (Zero-knowledge password proofs) metodas išverčia autentifikavimo ryšio seanso dalyvio slaptažodį į ilgą dvejetainį skaičių. Šis pakeitimas paslepia tikrąjį slaptažodį nuo jo gavėjo (serverio) ir pastarasis turi pateikti savo slaptažodžio versiją. Jei abiejų ryšio seansų dalyvių dvejetainiai skaičiai sutampa kliento autentifikacija būna patvirtinta išvengiant tiesioginio slaptažodžio siuntimo neapsaugotu kanalu.[23]

2.19 Parinkti sprendimo kūrimo metodai ir priemonės

Bankinių apmokėjimų sistemai visapusiškai apsaugoti, būtina naudoti keleto tipų priemones, kurios pilnai išspręstų saugumo problemas bei užtikrintų nepertraukiamą sistemos veikimą

1. Įsilaužimas tiesiogiai į tinklalapį

   Sprendimo metodas:

   - Prisijungimui prie el. parduotuvės tinklapio administravimo srities bus skirtas tik vienas IP bei vienas MAC adresas. Naudojamas slaptažodis privalės būti aštuonių simbolių ilgio, jis automatiškai tūrės būti pakeistas kas 7d. Šis sprendimas bus įgyvendinamas PHP programavimo kalba, nes visi tinklapio komponentai sukurti naudojant šią programavimo kalbą.

2. SMS žinutės perėmimas GSM ryšiu ir nuskaitymas „bluetooth“ ryšiu

   Sprendimo metodas:

   - SMS trumposios žinutės perėmimas, kai bankas siunčia pranešimą apie apmokėjimą, yra gan sunkiai apsaugomas todėl šioje vietoje būtina patobulinti A5 šifravimo algoritmą. Šiuo metu šis algoritmas yra nesunkiai įveikiamas dėl pakankamai nesudėtingos veikimo struktūros. SMS perėmimas kai „Bluetooth“ ryšiu duomenys siunčiami į sistemą, būtina naudoti aparatinį sujungimo kabelį, kurio pagalba išvengsime duomenų vagystės

3. Informacijos perėmimas sistemos kompiuteryje

   Sprendimo metodas:

   - Nuolat atnaujinama programinė įrangą
   - Naudojama aparatinė ugniasienė
   - Prisijungimui prie operacinės sistemos naudojami sudėtingi slaptažodžiai
   - Naudojama naujausia antivirusines programas versija
   - Kompiuteris naudojamas tik sistemos eksploatavimui
   - Kompiuterio aparatinė įranga laikoma stebimoje patalpoje, apsaugotoje nuo nesankcionuotos prieigos.
   - Autentifikacija jungiantis prie Bankinių apmokėjimų sistemos, reikalaujant 8 simbolių slaptažodžio bei papildomų duomenų pateikimo (vardas, pavardė, atsakymas į klausimą) bei atsitiktinio sugeneruoto sistemos kodo, kuris išsiunčiamas prieš kiekvieną prisijungimą administratoriui į el.paštą.

   Šis sprendimas bus įgyvendintas su C# programavimo kalba, nes sistema sukurta naudojant C# technologiją.

4. Informacijos perėmimas siunčiant nekoduotus duomenis tinklu

   Sprendimo metodas:

   Bankinių apmokėjimų sistemos pranešimų apsaugojimui naudojamos VPN tinklo sudarymas. Tai užtikrina koduotų duomenų siuntimą. VPN naudojami saugumo protokolai:

   - IPSec - padeda apsaugoti duomenis tinkle naudojant saugos tarnybas ir skaitmeninius sertifikatus kartu su viešaisiais ir privačiaisiais raktais.
   - SSL - **SSL** (*Secure Sockets Layer*) – kriptografinis protokolas, skirtas informacijos, sklindančios internete apsaugojimui šifruojant.[10]

Dėl VPN nepakankamo “end-point security” tikrinimo sistema nėra saugi, todėl virtualiame tinkle keliaujantys duomenys gali būti perimti. Šiai problemai išspręsti bus panaudojama SSH technologija. Susijungimas tarp dviejų duomenų bazių užmezgamas per VPN tunelį, kuriame duomenys siunčiami SSH tunelio pagalba.

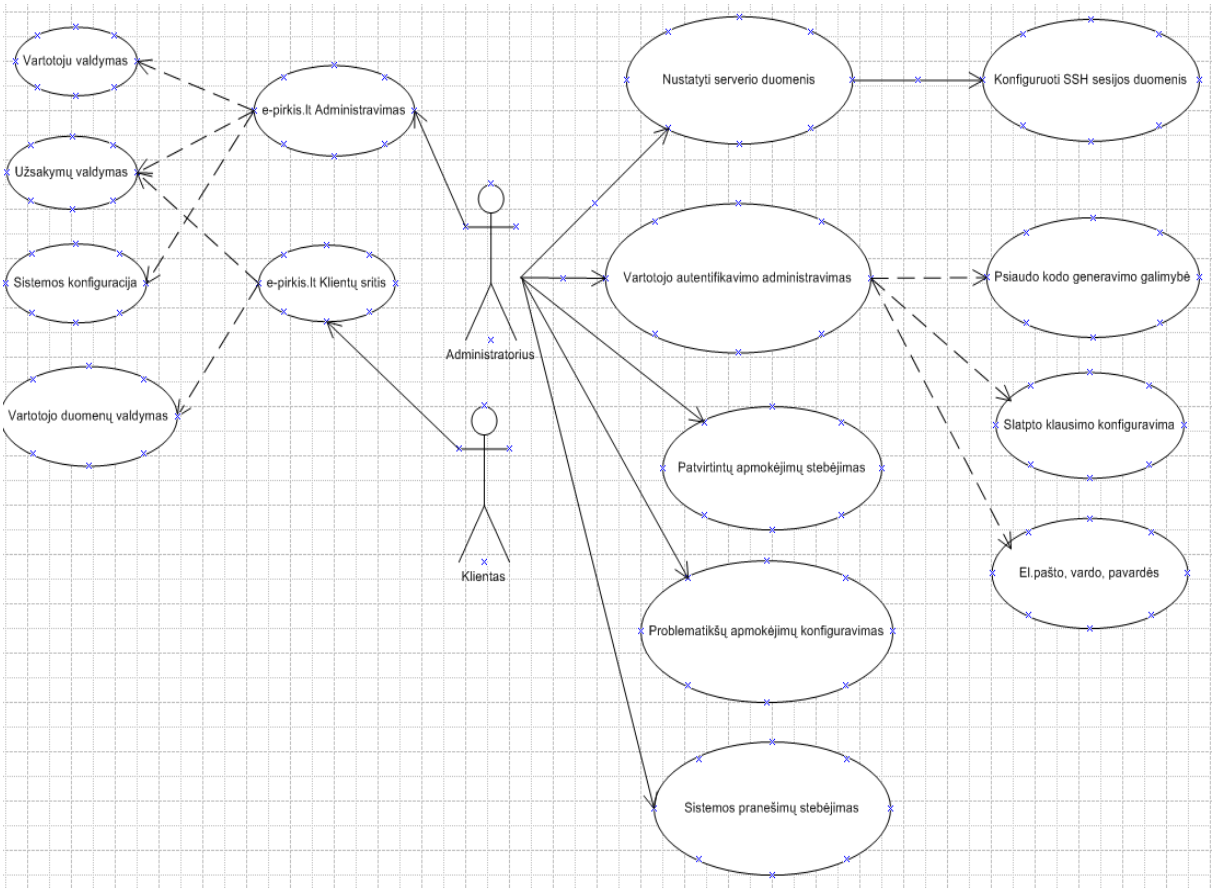
Saugumo spraga	Pažeidžiamumo lygis	Saugos priemonės
Įsilaužimas tiesiogiai į tinklalapį	Aukštas	Prisijungimui prie tinklapio el.prekybos sistemos administravimo srities bus skirtas tik vienas IP bei vienas MAC adresas. Naudojamas slaptažodis privalės būti 8 simbolių ilgio, jis automatiškai tūrės būti pakeistas kas 7d.
SMS žinutės nuskaitymas „bluetooth“ ryšiu	Žemas	Patikimas „bluetooth“ įrenginių identifikavimas arba telefono prijungimas per kabelį.
Informacijos perėmimas sistemos kompiuteryje	Aukštas	Autentifikacija jungiantis prie Bankinių apmokėjimų sistemos. Ugniasienės, antivirusinės programos, įsibrovėlių aptikimo sistemos.
Informacijos perėmimas siunčiant nekoduotus duomenis tinklu	Aukštas	**VPN bei SSH technologijų sujungimo panaudojimas**
SMS žinutės nuskaitymas pasinaudojant A5/1 spragomis	Žemas	Naudoti papildomas saugumo priemones

3 lentelė. Saugumo grėsmių įvertinimo bei sprendimų lentelė

2.20 Išvados:

- Išanalizavus visas „Free e-pay“ sistemos saugumo spragas buvo parinkti saugos įgyvendinimo sprendimai, padėsiantys užtikrinti šios sistemos saugumą.
- Pasirenkant VPN ir SSH technologijų sujungimą buvo išanalizuotos abi technologijos, tyrimas parodė, kad šios technologijos nėra visiškai saugios todėl į VPN tunelį siunčiant šifruotus duomenis padidinamas jų saugumas.
- Autentifikavimo metodų analizė parodė, kad sistema šiuo požiūriu nėra saugi, todėl buvo pasirinkta sustiprinti sistemos administratoriaus autentifikavimo priemones.

3 Bankinių apmokėjimų pranešimų saugos projektas



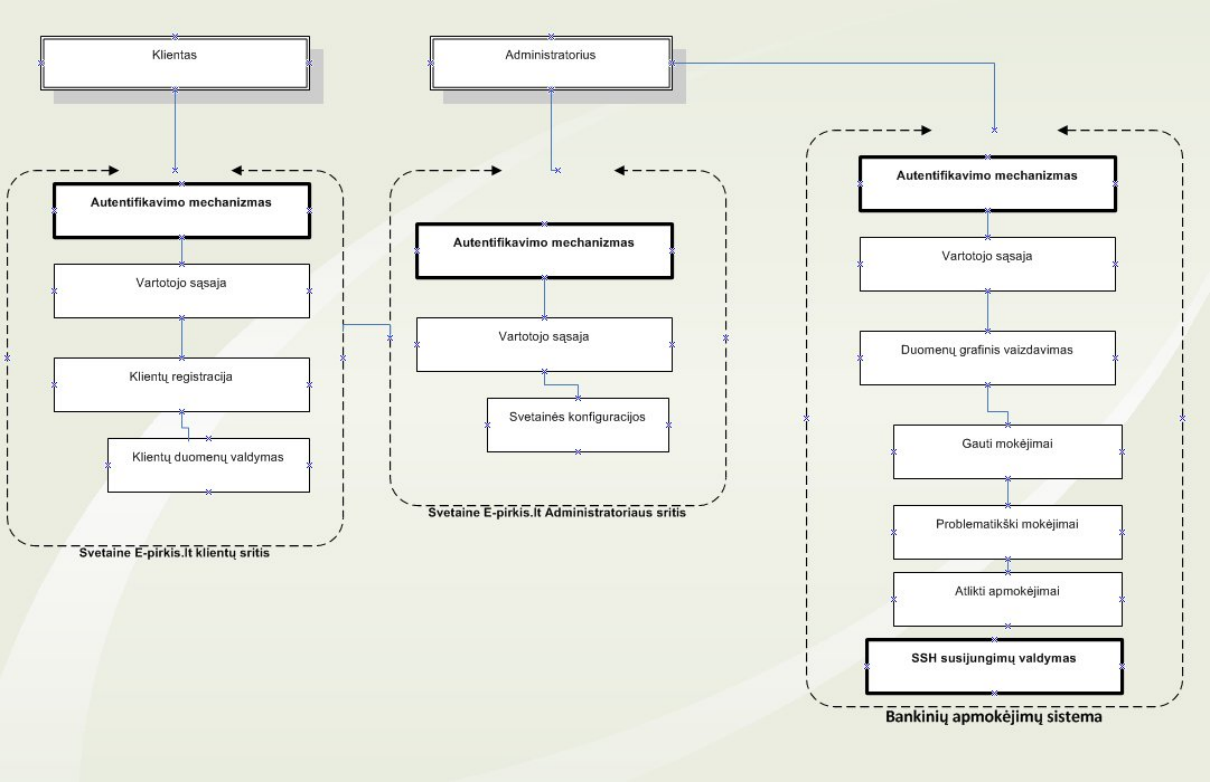
5 pav. „Free e-pay“ sistemos panaudos atvejų diagrama

Panaudojimo atvejų diagrama parodo, kokius veiksmus gali atlikti atskiro lygio vartotojas. Pateiktoje diagramoje (6pav.) brūkšniuota linija detalizuoja ką konkrečiai gali peržiūrėti vartotojas paspaudęs nurodyta komponentą. Privilegijuotas vartotojas administratorius gali konfigūruoti Bankinių apmokėjimų sistemos SSH serverio duomenis, nustatyti IP adresą, prisijungimo vardą, slaptažodį bei kitus parametrus. Prisijungus prie sistemos galima stebėti keletą informacinių laukų, kurių aprašymai pateikti lentelėje.

Prototipo grafinės vartotojo sąsajos komponentas	Paskirtis
ATLIKTI APMOKĖJIMAI	Peržiūrėti korektiškus apmokėjimus
PROBLEMATIŠKI APMOKĖJIMAI	Peržiūrėti nekorektiškus apmokėjimus
PRANEŠIMAI	Peržiūrėti pranešimus apie programos veikimą
SIUNTŲ ADRESAI	Šioje dalyje galima matyti korektiškų užsakymų adresus, kurie reikalingi siuntų ruošimui
ATLIKTI APMOKĖJIMAI	Peržiūrėti korektiškus apmokėjimus

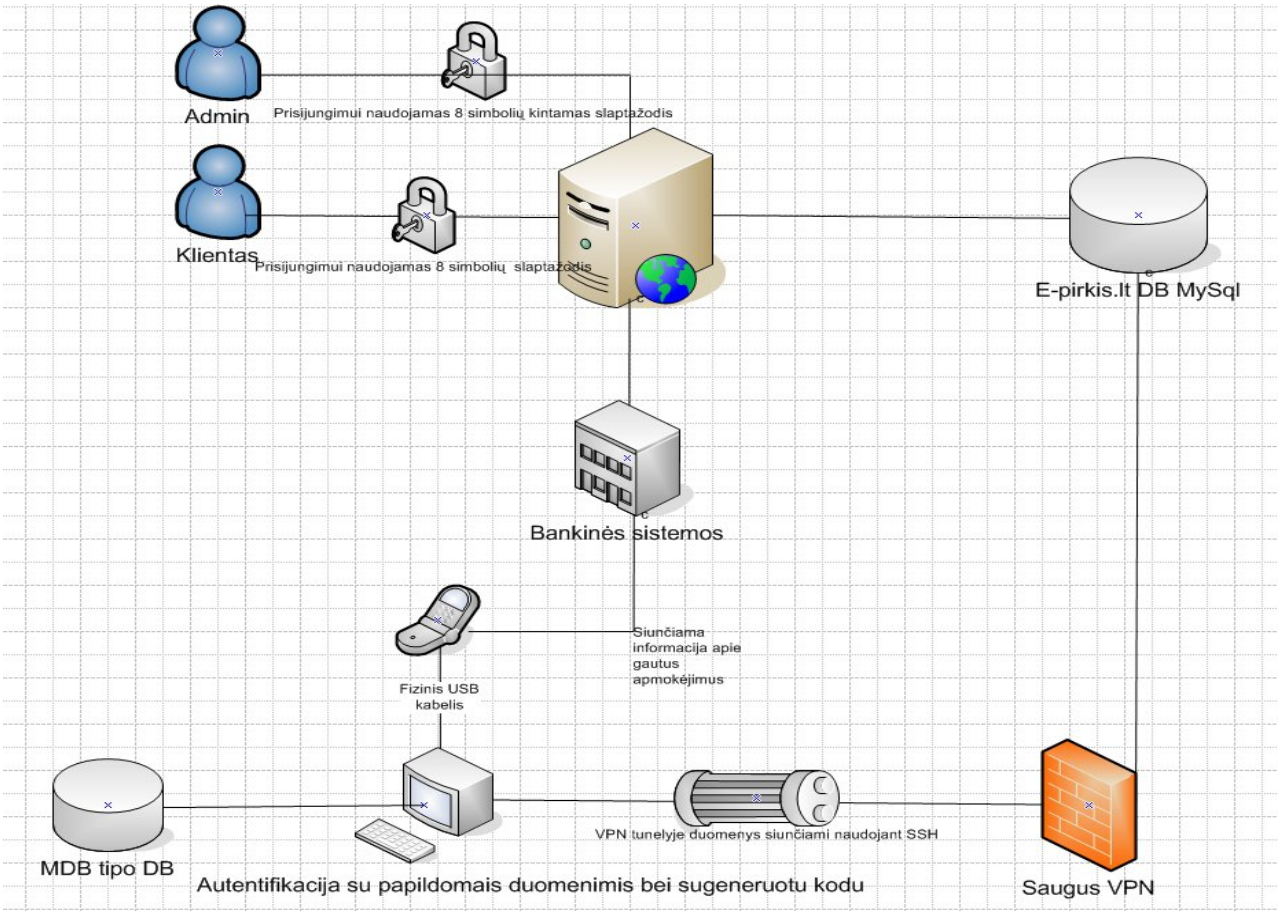
4 lentelė. Tekstinių laukų paskirties aprašymas

Sistemos komponentų bei funkcijų modelis:



6 pav. Sistemos komponentų bei funkcijų bendroji diagrama

Sistemos komponentų modelyje pavaizduoti sistemą sudarantys komponentai, vartotojai, bei jų tarpusavio ryšiai, bei funkcijos, kurias atskiri vartotojai sistemoje gali vykdyti.



6pav. Saugios „Free e-pay“ sistemos modelis

Pagrindinė „Free e-pay” sistemos saugos grėsmė: nekoduotų duomenų siuntimas internetu buvo išspręsta sujungus dvi duomenų šifravimo technologijas t.y. VPN ir SSH. Sukurtas VPN tunelis tarp „Free e-pay” serverio ir nutolusios duomenų bazės sukūrė saugų duomenų perdavimą, tačiau dėl VPN naudojamų protokolų saugos trūkumų duomenys iš VPN tunelio gali būti perimti todėl buvo pasirinkta, kad tuneliavimo metu duomenys bus siunčiami SSH technologijos pagalba. Taip išvengiant duomenų iššifravimo ir pakeitimo VPN tunelio pažeidimo atveju. Programiškai yra naudojamos jau sukurtos VPN ir SSH bibliotekos duomenų šifravimui įgyvendinti.

3.1 Saugumo komponentų grafinės savybės bei aprašymai:

8 pav. Bankinės sistemos autentifikavimo komponento grafinis vaizdas

Šis autentifikavimo komponentas įdiegtas į bankinių apmokėjimų sistemą ir aktyvuojasi jungiantis prie jos. Administratorius privalo įvesti prisijungimo vardą, slaptažodį, savo vardą pavardę, bei sugeneruotą pseudo kodą, kuris yra atsiunčiamas į el.paštą

9 pav. Tinklapio autentifikavimo komponento grafinis vaizdas

9 paveiksle pavaizduotas prisijungimas prie el. komercijos sistemos su papildoma saugumo funkciją, slapta fraze, kurią administratorius turi įvesti prieš įsiregistruodamas į sistemą

3.2 Išvados:

Įgyvendinus „Free e-pay“ sistemos saugumo priemones, pavyko padidinti sistemos saugumą bei apsaugoti sistemą nuo duomenų nesankcionuoto panaudojimo. Siunčiami duomenys šifruojami dviguba VPN ir SSH technologija. Pagerinus autentifikavimo priemonių veikimą buvo užtikrintas saugus priėjimas prie sistemos naudojimo. Išsprendus aparatines sistemos saugumo spragas buvo pagerintas sistemos patikimumas, ko pasėkoje sistema dirba stabiliau bei našiau.

4 Sistemos testavimas

Dėl pakankamai didelių duomenų kiekių, bei testavimo tipų, visi sistemos testavimo bei eksperimentavimo darbai atlikti su OPNET IT GURU programiniu paketu. Darant eksperimentus buvo ištirti kritiniai bei silpniausi sistemos taškai. Atliekant testavimo darbus buvo išsiaiškinta papildomų sistemos problemų.

Tiriant sistemos patikimumą buvo atsižvelgta į pagrindinius sistemos vienetus, serverio apkrovimą, duomenų bazės apkrovimą, Bankinių sistemos pranešimų serverio apkrovimą.

Tiriant sistemos saugumą buvo atsižvelgta į šiuolaikines tinklo atakas, tinklo apkrovimą, tinklo topologiją. Norint palyginti sistemos saugumą prieš ir po saugumo įdiegimo buvo išnagrinėti dviejų tipų tinklai, su saugumo parametrais ir be jų.

4.1 „Free e-pay“ sistemos testavimo tikslai

- Ištestuoti atskirų sistemos dalių veikimą, imituojant atakas prieš jas.
- Ištestuoti sistemos saugą, tinklo atakos metu.
- Ištestuoti VPN technologijos duomenų šifravimo vėlinimą ir įtaką sistemos veikimui.

4.2 Sistemos paruošimas testavimui

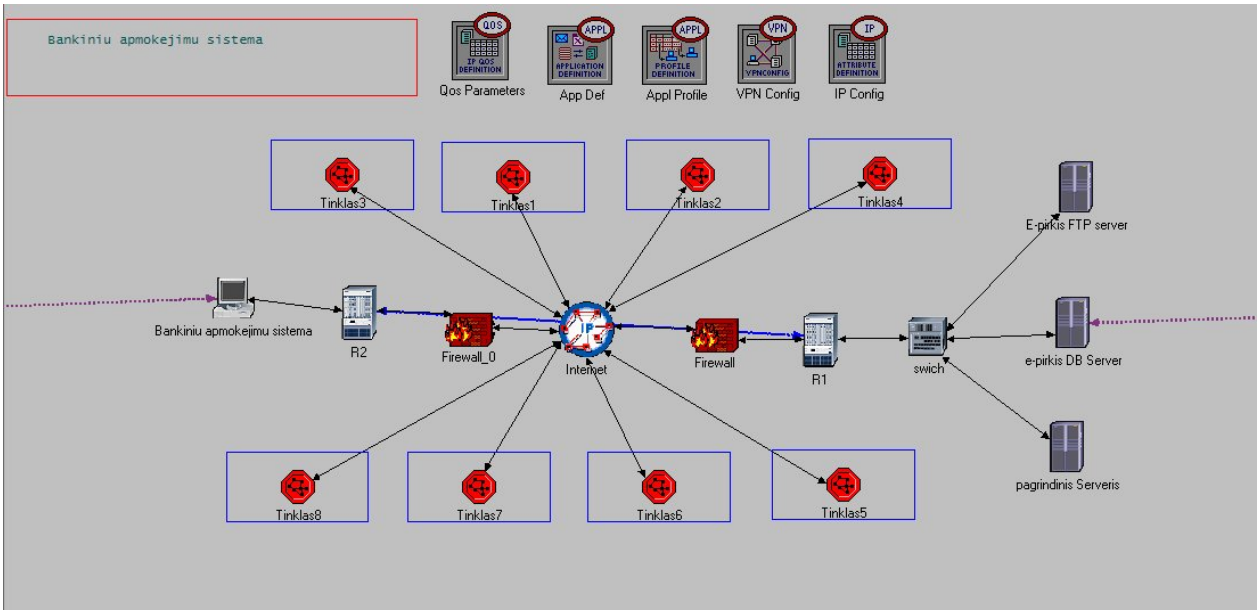
OPNET IT GURU programinis paketas yra laisvai platinamas moksliniams tikslams bei tyrimams. Sistemos paruošimas darbui nereikalauja ypatingo dėmesio bei konfigūracijos. Po programinio paketo įdiegimo bei konfigūravimo atlikti eksperimento paruošiamieji darbai:

- Susipažinimas su Opnet sistema
- Tinklo topologijos sukūrimas
- Tinklo elementų konfigūravimas
- Tinklo ryšių nustatymas bei konfigūravimas
- Rezultatų ataskaitų sukonfigūravimas [13]
- Rezultatų vaizdinių priemonių sukonfigūravimas

4.3 „Free e-pay“ sistemos tinklo topologijos sudarymas

4.3.1 Sistemos tinklo modeliavimas OPNET IT GURU programiniu paketu

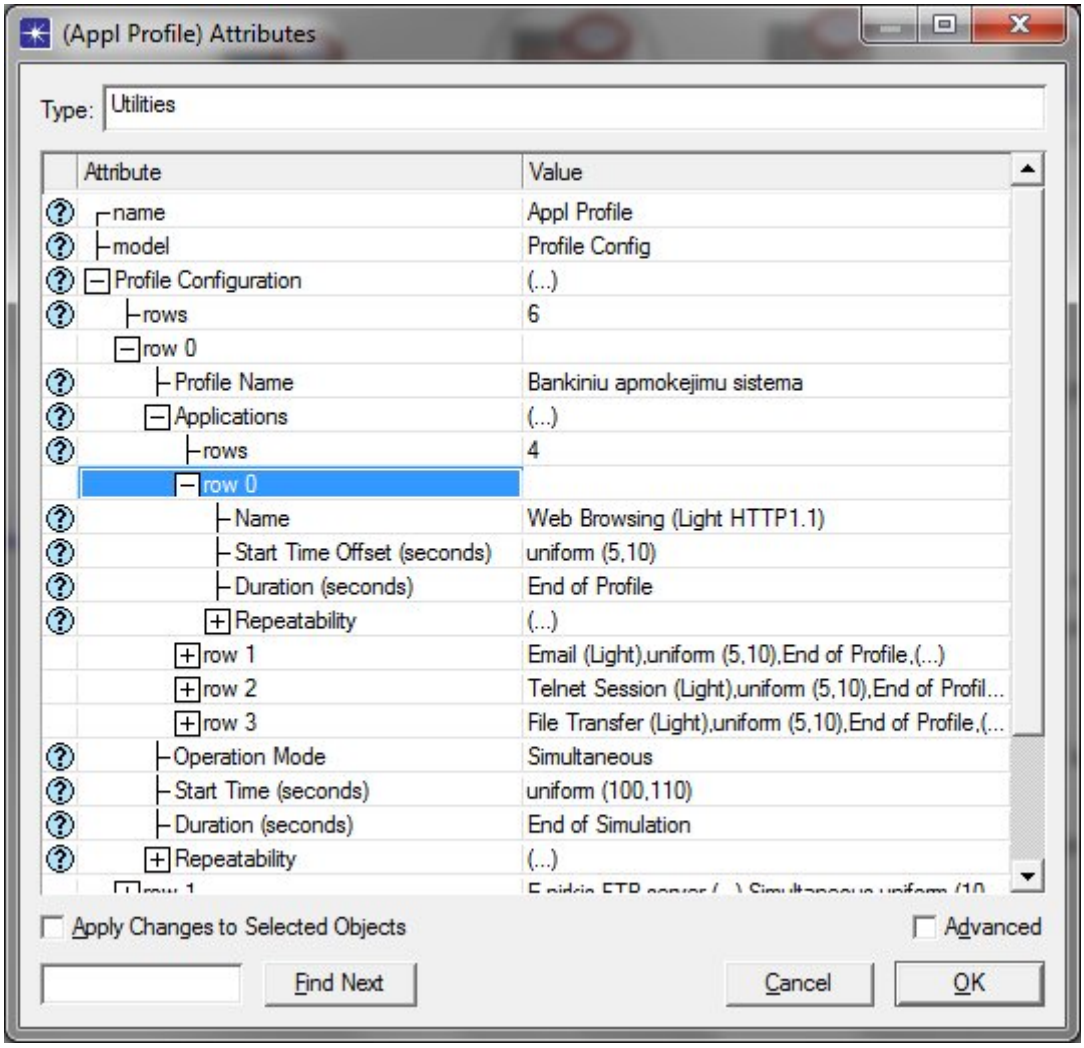
Tinklo topologijos sudarymui panaudoti duomenys iš sistemos aprašymo dalies. Pasirinkta identiška tinklo elementų struktūra taip pat kiekvienas sistemos elementas fiziškai išskirtas į atskirą serverį, tačiau realiai jie yra viename tinkle. Pasitelkiant OPNET IT GURU programinio paketo galimybėmis nustatyti ryšiai tarp elementų bei sukonfigūruoti reikiami tinklo parametrai[20]. Tarnybinėse stotyse buvo nustatytos paslaugos, kokias teikia atskira tarnybinė stotis. Vienoje nustatyta HTTP paslauga, kitoje FTP, trečioje DB.



10pav. Bankinių apmokėjimų sistemos schema OPNET IT GURU programiniame pakete

4.4 Opnet IT GURU teikiamų paslaugų konfigūravimas

Kiekvieno programinio paketo schema OPNET IT GURU komponento paslaugas galima apibrėžti Application_config paslaugų nustatymo modulyje. Nustatytos visos paslaugos, kurios teikiamos tinkle, bei nustatytas jų apkrovimas.



11pav. Application_config paslaugų konfigūravimo langas

4.5 „Free e-pay“ sistemos testavimo metodai

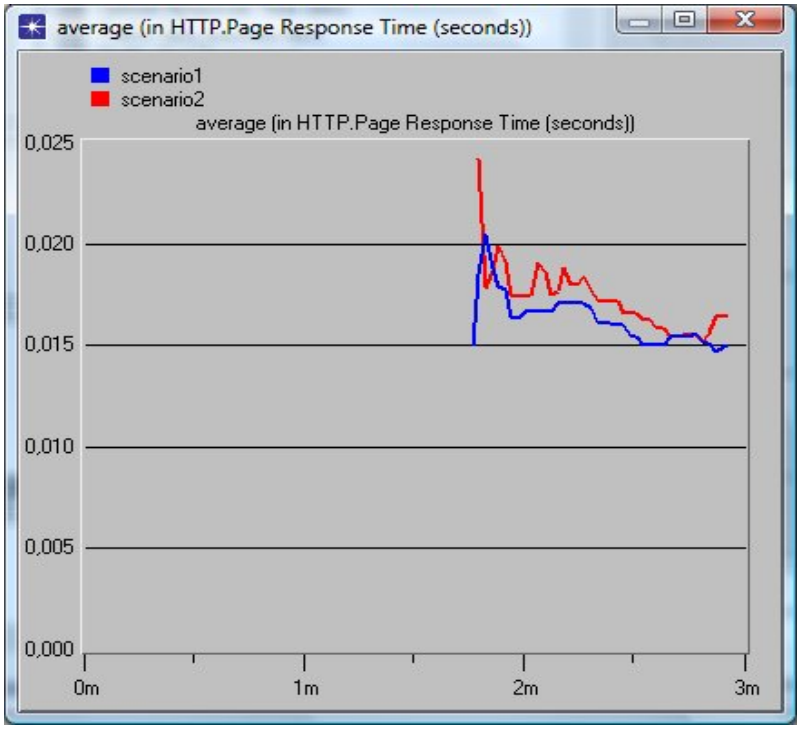
- Sistemos duomenų perdavimo patikimumo testavimas.
- Sistemos saugumo testavimas.

4.6 Sistemos duomenų perdavimo patikimumo testavimo scenarijus

Sistemos duomenų perdavimo patikimumo testavimui ištirti buvo pasirinkti keli kokybės parametrai tinkle, kurie parodo sistemos veikimą kritiniais momentais. Ištiriant sistemos patikimumą pasirinkti šie parametrai:

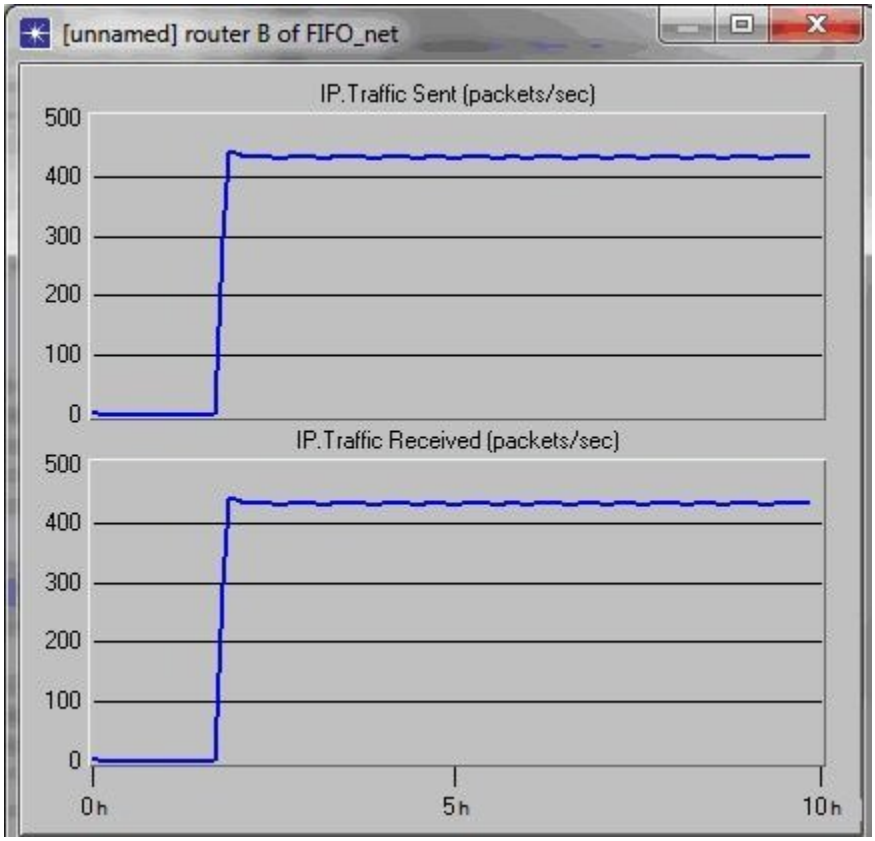
- Duomenų persiuntimo vėlavimas, siunčiant duomenis VPN tuneliu
- Duomenų persiuntimo kokybės parametrų nustatymas.

HTTP kokybės charakteristikas parodantis grafikas, Scenario1 tai tinklas be VPN tunelio, o scenario2 tai tinklas su VPN tuneliu.



12pav. Kokybės charakteristikas parodantis grafikas

Grafike matomos dvi kreivės atspindi HTTP duomenų persiuntimo laiką, kai duomenys tinkle siunčiami su VPN tuneliu ir be VPN tunelio. Iš grafiko matome, kad sistemos atsako laikas išauga kai naudojamas VPN tunelis, tai paaiškinama dėl pačios VPN architektūros, kai duomenys tunelyje užkoduojami ko pasėkoje išauga duomenų persiuntimo laikas.



13pav. Sistemos siunčiamų IP paketų išsiuntimo bei gavimo diagrama

Persiunčiant duomenis tinklu labai svarbu, kad tinklo darbas nesutriktų to pasekoje išliktų stabilus paketų perdavimas visą sistemos veikimo laiką. Quality of Service parodo sistemos nepertraukiamumą, kai duomenys išsiunčiami ir gaunamas atsakymas. 13 paveiksle matomas išsiųstų ir gautų paketų kiekis per sekundę. Per dešimt sistemos veikimo valandų pamestų paketų skaičius yra praktiškai lygus nuliui. Ištyrus tinklo QoS, nustatyta, kad tinklo kokybės parametras arti 100%.

4.7 Sistemos saugumo testavimo scenarijus

Tiriant sistemos saugumą daug dėmesio skirta nesankcionuotam sistemos paveikimui, bandant prisijungti „nulaužiant“ slaptažodį ar sukeliant DoS ataką.[17] Tinklo sauga labai priklauso nuo tinkle veikiančių fizinių saugos elementų, todėl pasirinktas tinklo saugos modelis su ugniasiene. [18].

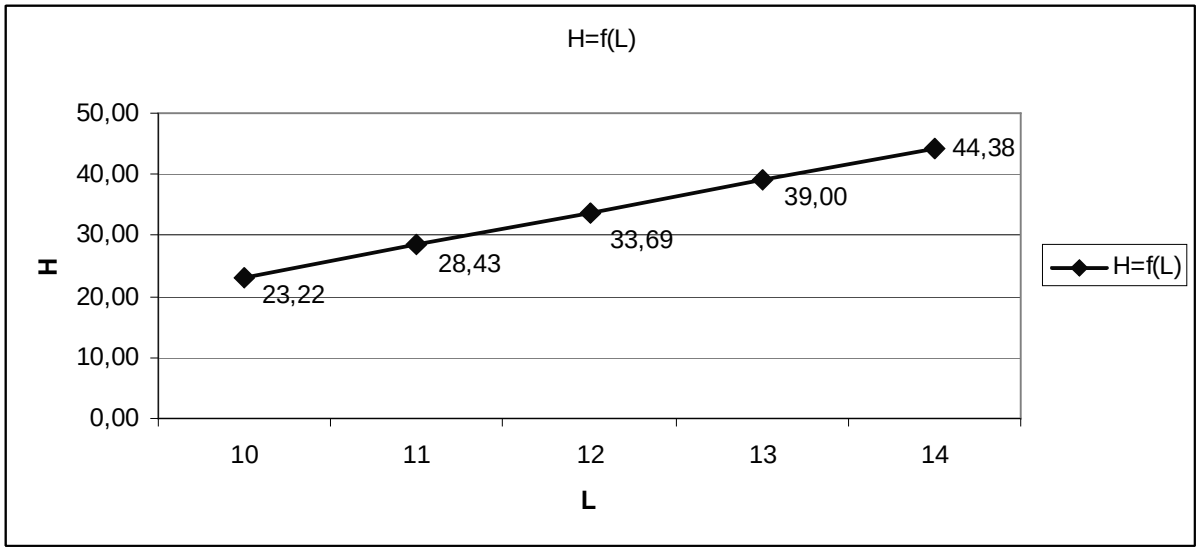
Tiriant sistemos tinklo saugą pasirinkti šie parametrai:

- TVS administracijos slaptažodžio nulaužimas
- DoS ataka prieš DB serverį
- VPN tunelio end-point apkrovimas ICMP užklausomis.
- Tinklo veikimo parametrai. DoS atakos metu.

4.8 Slaptažodžio stiprumo bei patikimumo tyrimas

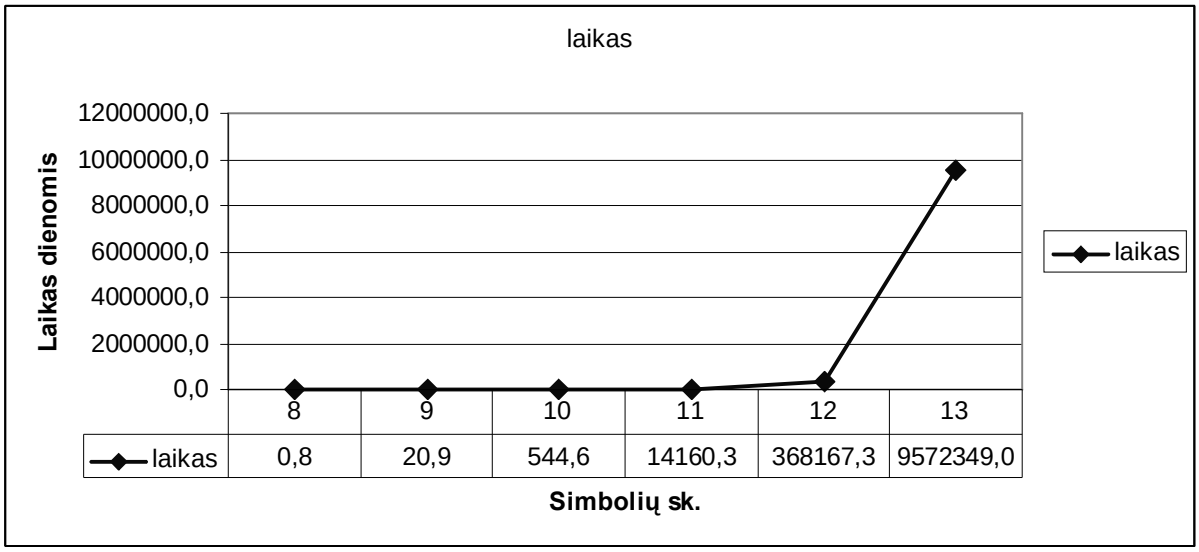
Slaptažodžio stiprumas H, logaritmiškai priklauso nuo simbolių skaičiaus L, bei skirtingų galimų simbolių skaičiaus N. Skaičiavimai atlikti naudojant formulę:[11]

$$H = L \log_2 N = L \frac{\log N}{\log 2}$$



14pav. Slaptažodžio stiprumo tyrimo grafikas

Didėjant slaptažodžio simbolių skaičiui ir galimų skirtingų simbolių skaičiui slaptažodžio stiprumas didėja. Slaptažodžio stiprumas priklauso ir per kiek laiko *t* bus „nulaužtas“ slaptažodis, kai slaptažodį sudarančių simbolių skaičiaus kitimo ribos yra *L*, o galimų skirtingų simbolių skaičius yra *N*, jei turimas kompiuteris per sekundę gali sugeneruoti *D(3mln/sek)* slaptažodžio variantų. Grafinė priklausomybė $t = f(L)$ pavaizduota grafike.



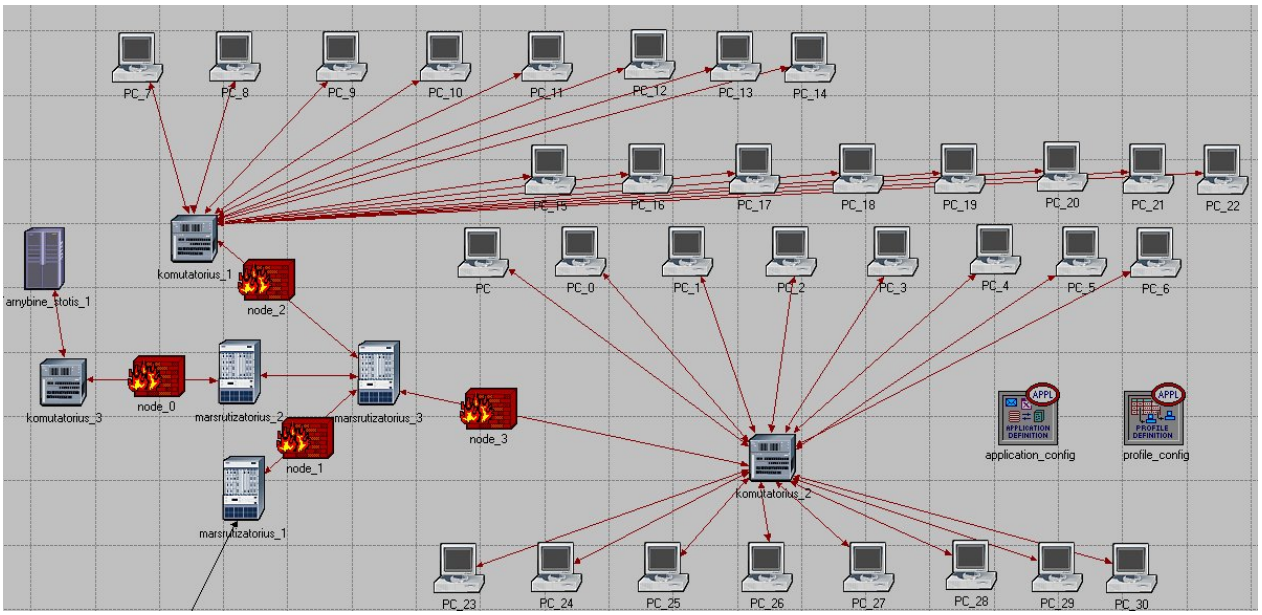
15pav. Slaptažodžio nulaužimo laiko priklausomybė nuo simbolių skaičiaus

Iš grafiko matome, kad didėjant slaptažodžio ilgiui L, nulaužimo laikas labai išauga, kadangi kompiuterio procesoriaus atliekamų operacijų skaičius 3mln./sec. Nustatyta, kad sistemos TVS aštuonių simbolių slaptažodis parinktas per mažas tačiau kadangi sistemoje parinktos kelios papildomos taisyklės slaptažodžio įvedimui (pseudo kodo generavimas) sistemos saugumas nesumažėja.

4.9 DoS atakos simuliavimas

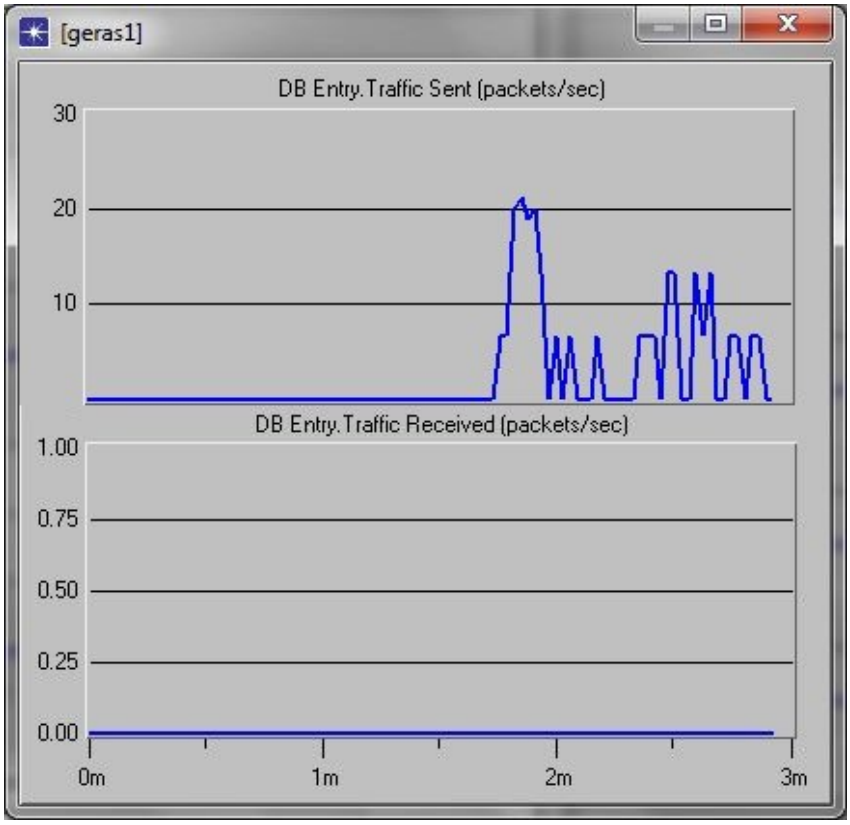
DoS (denial of service) [12]- atkirtimo nuo paslaugos ataka. Atakos tikslas - paveikti kompiuterinę sistemą arba tinklą taip, kad kompiuterinės paslaugos taptų neprieinamos vartotojams. DoS atakos metu gali būti perkraunami kompiuteriniai resursai (perpildomas tinklas, apkraunama atmintis ar CPU). „Free e-pay” sistemos pažeidžiamiausia vieta yra pagrindinis sistemos serveris, kuris prijungtas prie interneto ryšio ir atsakingas už apmokėjimų apdorojimą.

Testavimas atliekamas kai duomenų srautas nėra siunčiamas VPN tuneliu. Šiam serveriui apkrauti panaudoti aštuoni fiziniai tinklai, kiekvienas iš jų turi trisdešimt du vartotojus. Iš kiekvieno vartotojo į „Free e-pay" sistemos serverį siunčiamos ICMP užklausos 1000 paketų per sekundę iš kiekvieno vartotojo, to pasėkoje serverio darbas sutrinka ir dėl atsiradusių trukdžių sistema nustoja veikusi.[21], [19]



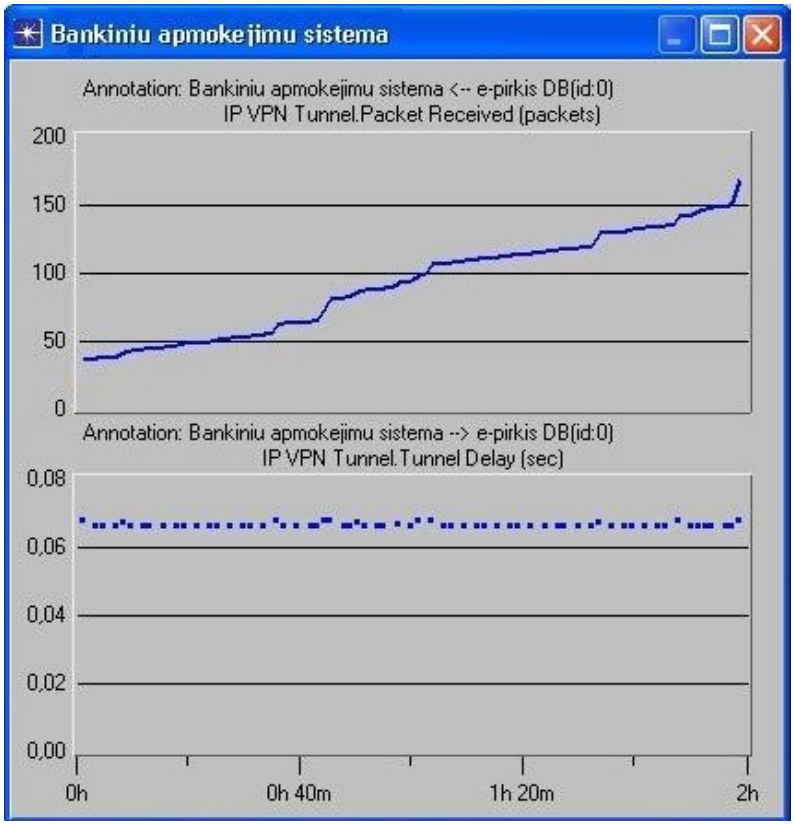
16 pav. Vieno iš aštuonių fizinių tinklų schema

Apkrovus serverį ICMP užklausomis duomenų bazės atsako laikas labai išaugo, ko pasėkoje sistemos darbas sutriko. Šis sistemos veikimo sutrikimas kritinis, nes tai įtakojo visos sistemos nefunkcionavimą.[16]



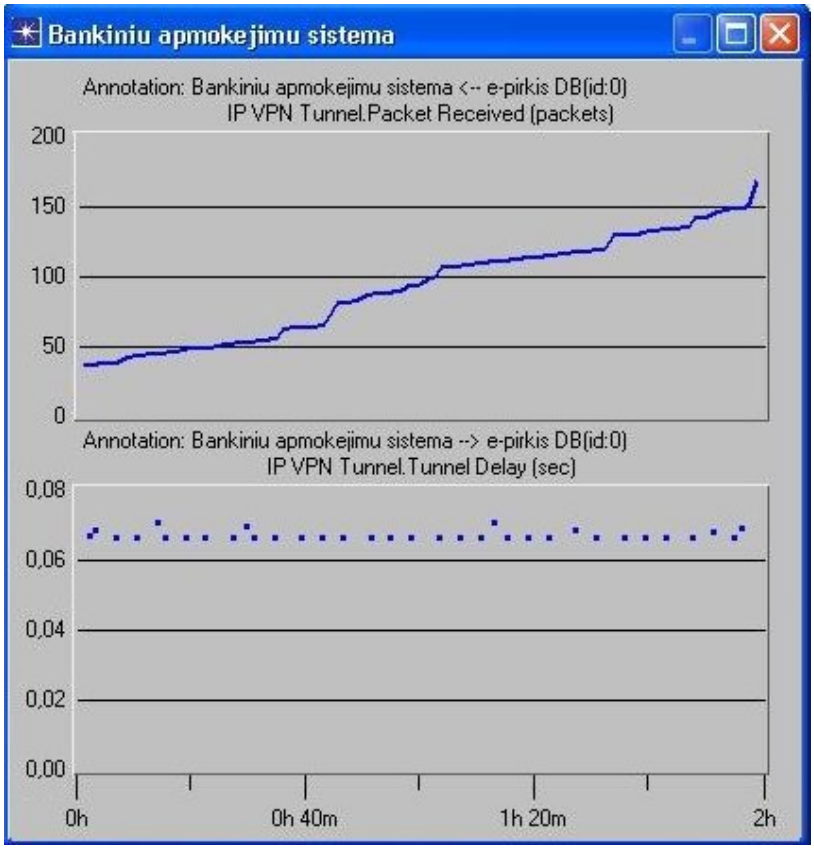
17pav. Duomenų bazės duomenų siuntimo gavimo grafikas

Įdiegus į „Free e-pay" sistemą papildomų saugumo priemonių, nežymiai pasikeitė tinklo parametrai. Sistemos duomenų perdavimui naudojant VPN tunelį, duomenų perdavimo greitis sumažėjo dėl šifravimo, dešifravimo funkcijų įvykdymo, tačiau sistemos duomenys tinkle buvo siunčiami šifruoti to pasekoje sistemos saugos lygis stipriai išaugo. Kadangi nepriklausomai ar duomenys šifruoti ar ne DoS tipo atakos gali būti panaudotos galutiniam (end-point) VPN taškui, dėl to sutrinka VPN tunelio našumas. Testuojant tinklą su VPN tuneliu buvo apkrautas galutinis taškas – išorinė duomenų bazė. VPN buvo sukonfigūruotas „compulsory tunneling" rėžimu bei naudojo L2TP technologiją.



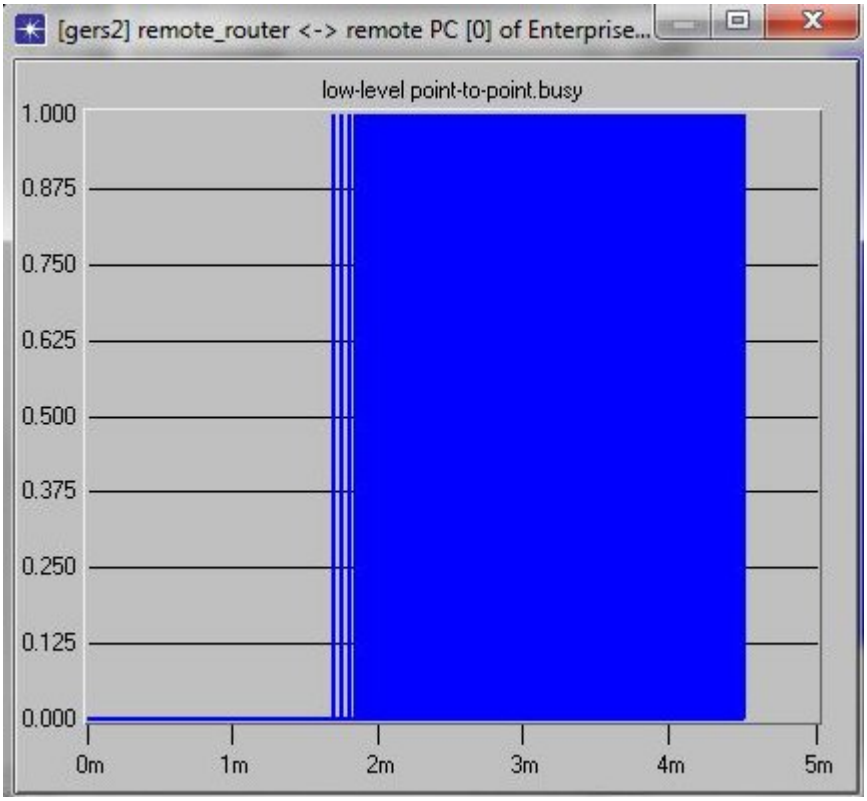
18pav. VPN tunelio parametrai DoS atakos metu

Palyginimui 19 paveiksle pateikiamas grafikas kai „Free e-pay“ sistema nebuvo atakuojama DoS ataka. Išanalizavus grafiką matosi kad VPN tunelio paketų siuntimo laiko parametrai yra žymiai geresni nei DoS atakos metu. Dėl VPN tunelio architektūros duomenys tinkle yra saugūs, tačiau dėl galimybės atakuoti bei suklastoti galutinio taško prieigą, duomenys gali būti perimti. Šiuo atveju norint apsaugoti duomenis būtina naudoti papildomą saugos priemonę SSH technologiją. Dėl Opnet IT GURU licenzijos apribojimų, tinklo topologijos sudarymas, kai VPN tuneliu siunčiami duomenys SSH pagalba yra neįmanoma, todėl sistemos saugumo lygio esant tokiai konfigūracijai ištestuoti galimybės nėra.



19pav. VPN tunelio parametrai, kai DoS ataka nenaudojama

Dėl DoS atakos įtakos apkraunamas visas tinklas (20pav.) todėl tinklo kokybės parametrai suprastėja, dėl šios priežasties gali būti pažeidžiamas tinklo saugumas, nes kritinio apkrovimo metu tinklo maršrutizatoriai nespėja atsakyti į tinklo užklausas ir to pasėkoje duomenų perdavimas tinkle sutrinka. Norint išvengti didelių apkrovų būtina naudoti pažangią tinklo įrangą, kuri sugeba atpažinti ir blokuoti nepageidaujamą srautą. Tinklą saugančios ugniasienės atlieka svarbų vaidmenį tinklo saugume, todėl būtina jas sukonfigūruoti tinkamai ir jų programinę įrangą atnaujinti reguliariai.[17]



20pav. Tinklo užimtumas DoS atakos metu

4.10 Sistemos testavimo rezultatų išvados

Ištestavus sistemą su OPNET IT GURU programiniu paketu, galima teigti, kad išanalizuotos ir nustatytos sistemos veikimo silpnosios bei stipriosios pusės. „Free e-pay“ sistemos veikimas ištestuotas kritinėse tinklo saugumo situacijose. Testavimo metu nustatyta, kad dėl duomenų šifravimo ir dešifravimo, perdavimo sparta yra mažesnė nei siunčiant duomenis nešifruotus, tačiau dėl nedidelių vėlinimų, sistemos darbui, tai įtakos neturi. Ištyrus VPN tunelio apkrovimą DoS atakos metu nustatyta, kad paketų vėlinimo laikas yra išaugęs, tačiau paketų perdavimo kokybė nepasikeitusi. Testuojant tinklo maršutizatorių apkrovą buvo nustatyta, kad tinklas yra pilnai apkrautas, tačiau veikė stabiliai, tai parodo, kad tinklo įrenginiai yra kokybiški ir veikia stabiliai.

5 Išvados

Bankinių apmokėjimų pranešimų sistemų paplitimas bei lankstus pritaikymas, paskatino šių sistemų integraciją į verslą. Dėl piktavališkų veiksmų el.erdvėje, pasinaudojant bankinėmis sistemomis, iškilo daug saugos grėsmių, todėl šių sistemų saugos problemos sprendžiamos pasirenkant individualius, nestandartinius saugos sprendimus.

Atlikus tiriamąjį darbą, nustatyta:

1. Bankinių apmokėjimų pranešimų sistemų analizė parodė, kad kiekviena sistema turi trūkumų ir nėra visiškai saugi.
2. Atlikta kiekvienos bankinės apmokėjimų sistemos silpnų vietų analizė ir nustatytos grėsmės.
3. Bankinių pranešimų saugos sistemai „Free e-pay“ pritaikyti individualūs saugumo sprendimai, saugos politikai įgyvendinti
4. VPN ir SSH technologijų panaudojimas, pasiteisino „Free e-pay“ sistemos duomenų perdavimo saugai įgyvendinti.
5. Opnet IT Guru programinio paketo pagalba sumodeliuotas „Free e-pay“ sistemos tinklo modelis, kuris padėjo išsiaiškinti saugumo priemonių atsparumą atakoms.
6. Tyrimo metu atskleisti sistemos „Free e-pay“ trūkumai, sistema ištestuota kritinėmis veikimo sąlygomis.

6 Literatūra

[1] Munir Kotadia, Check Point Plugs VPN security hole. [žiūrėta 2009-01-20]. Prieiga per internetą: http://news.zdnet.com/2100-1009_22-137488.html

[2] Microsoft, MSDN Library, Virtual Private Networks. [žiūrėta 2009-01-18]. Prieiga per Internetą: http://msdn.microsoft.com/en-us/library/aa503420.aspx

[3] WIKIPEDIA Library. Virtual private network. . [žiūrėta 2009-01-18]. Prieiga per Internetą: http://en.wikipedia.org/wiki/VPN

[4] Modestas Kapušinskas Referatas „Bluetooth“ sistemos saugumas, [žiūrėta 2009-03-14], Prieiga per internetą http://www.mokslai.lt/referatai/referatas/30253.html

[5] Gilbert Held. Virtual Private Networking: A Construction, Operation and Utilization Guide. [žiūrėta 2010-01-24]. Prieiga per internetą: http://books.google.com/books?id=AvHQfXHCAOQC&pg=PA22&dq=vpn#PPA18,M1

[6] Daniel J. Barrett, Richard E. Silverman. SSH, the secure shell: the definitive guide. Part 3.[žiūrėta 2010-01-24]. Prieiga per internetą: http://books.google.com/books?id=JFa5aLIII6oC&printsec=frontcover

[7] Charlie Kaufman, Radia Perlman, Mike Speciner, Michael Speciner Network Security. Private Communication in a Public World. .[žiūrėta 2010-01-24]. Prieiga per internetą http://books.google.com/books?id=JJqBw6f2beQC&printsec=frontcover&dq=network+security&ei=XSAzSoHXDIzqzASv5sCNBg#PPR7,M1

[8] Bradley Mitchell What Are the Advantages and Benefits of a VPN? .[žiūrėta 2009-11-03]. Prieiga per internetą http://compnetworking.about.com/od/vpn/f/vpn_benefits.htm

[9] VPN Consortium. VPN Technologies: Definitions and Requirements.[žiūrėta 2009-10-11]. Prieiga per internetą http://www.vpnc.org/vpn-technologies.htm

[10] Very Sign. Secure Sockets Layer, .[žiūrėta 2009-10-11]. Prieiga per internetą http://www.verisign.com/ssl/ssl-information-center/how-ssl-security-works/

[11] Wikipedia. Password strength.[žiūrėta 2010-02-11]. Prieiga per internetą http://en.wikipedia.org/wiki/Password_strength

[12] Mian Zhou and Sheau-Dong Lang .A frequency-Based Approach to Intrusion Detection, Part 3.1 Network Intrusion Simulation Using OPNET. [žiūrėta 2010-02-11]. Prieiga per internetą: http://www.iiisci.org/journal/CV$/sci/pdfs/P602668.pdf

[13] OPNET Technologies, Inc. OPNET online documentation 8.0. [žiūrėta 2010-02-11]. Prieiga per internetą: http://www.ensc.sfu.ca/people/faculty/ljilja/ENSC835/News/Presentations/ENSC835_opnet.pdf

[14] Tao Wan, Xue Dong Yang,"IntruDetector: A Software Platform for Testing Network Intrusion Detection Algorithms", in Proceedings of 17th Annual Computer Security Applications Conference, 2001.[žiūrėta 2010-03-08]. Prieiga per internetą: http://www.ccsl.carleton.ca/~twan/papers/tao-acsac01.pdf

[15] Wikipedia, Denial-of-service attack. [žiūrėta 2010-03-08]. Prieiga per internetą http://en.wikipedia.org/wiki/Denial-of-service_attack

[16] Net Master Class, LLC. A BRIEF DESCRIPTION OF AN ICMP FLOOD/SMURF ATTACK [žiūrėta 2010-03-09]. Prieiga per internetą https://www.netmasterclass.net/site/articles/A%20Brief%20Description%20of%20an%20ICMP%20Flood%20Attack.pdf

[17] Fu-Hau Hsu, Fanglu Guo. Network-based Buffer Overflow Attack Detection, [žiūrėta 2010-03-03]. Prieiga per internetą: http://www.ecsl.cs.sunysb.edu/~fanglu/buffer_overflow_detection.htm

[18] Sheau-Dong Lang. Network traffic simulation for intrusion detection. [žiūrėta 2010-03-09]. Prieiga per internetą http://www.cs.ucf.edu/~mzhou/OPNET_Research.htm

[19] Mohammad Heidari. The Role of Modeling and Simulation in Information Security The Lost Ring. [žiūrėta 2010-03-11]. Prieiga per internetą http://www.infosecwriters.com/text_resources/pdf/MandS_MHeidari.pdf

[20] Kevin Richardson, Harold W. Fletcher, Martin C.Carlisle, J.A Hamilton. EVALUATING SECURE OVERLAY SERVICES THROUGH OPNET SIMULATION. [žiūrėta 2010-03-11]. Prieiga per internetą http://www.eng.auburn.edu/users/hamilton/security/pubs/MGA016_SOS.pdf

[21] Agustin Zaballos, Guiomar Corral, Isard Serra, Jaume AbellaTesting Network Security Using OPNET. [žiūrėta 2010-03-24]. Prieiga per internetą http://www.salle.url.edu/~zaballos/opnet_interna/pdf/OPNET2003b.pdf

[22] Roman Chertov, Sonia ,Fahmy, Ness B. , ShroffShr. High Fidelity DoS Experimentation. [žiūrėta 2010-03-19]. Prieiga per internetą http://www.cs.purdue.edu/homes/fahmy/emist/june06/fidelity.pdf

[23] Richard E. Smith, Ph.D., CISSP. The Strong Password Dilemma. [žiūrėta 2010-01-14]. Prieiga per internetą http://www.cryptosmith.com/sanity/pwdilemma.html

[24] RSA, The Security Division of EMC. Enhanced User Authentication Techniques. . [žiūrėta 2010-01-14]. Prieiga per internetą. http://www.rsa.com/rsalabs/node.asp?id=3105

[25] Rainer Wichmann. Defending against brute force ssh attacks. [žiūrėta 2009-03-11]. Prieiga per internetą: http://www.la-samhna.de/library/brutessh.html

[26] Swedbank, AB. Swedbank Gateway. [žiūrėta 2009-10-15]. Prieiga per internetą: http://www.swedbank.lt/lt/pages/verslo/el_bankininkyste/swedbank_gateway

[27] SEB, AB. SEB BANK LINK. [žiūrėta 2009-10-15]. Prieiga per internetą http://www.seb.lt/pow/content/seb_lt/pdf/en/Bank_Link_Specification.pdf

7 Terminų ir santrumpų žodynas

DB – duomenų bazė.

HTTPS – hypertekstinis perdavimo protokolas naudojantis duomenų šifravimą.

SSL (*Secure Sockets Layer*) – kriptografinis protokolas

MySQL – viena iš reliacinių duomenų bazių valdymo sistemų.

DoS - Denial-of-service attack – tinklo ataka, kai sutrikdomas paslaugos ar serviso tiekimas kitiems vartotojams.

QoS – quality of service, paslaugos teikimo kokybės parametras.

PHP – Hypertext Preprocessor, dinaminių puslapių kūrimo kalba.

TVS – Turinio valdymo sistema.

C# - programavimo kalba.

VPN – virtualus privatus tinklas

SSH – secure shell, tinklo protokolas, aprašantis apsaugotą kliento prisijungimą prie serverio aplinkos.

8 Priedai

„Free e-pay“ sistemos įdiegimo bei panaudojimo pažyma.

SEIFNETA

UAB “SEIFNETA” įmonės kodas:300623299, PVM kodas:LT100004080619, Adresas: Šaulių 37, Marijampolė, LT-68282, Tel +37068330800, A/s. LT497181800003468518 Šiaulių bankas,

PAŽYMA

KAUNO TECHNOLOGIJOS UNIVERSITETUI
INFORMATIKOS FAKULTETO
KOMPIUTERIŲ KATEDRAI

2010.05.28
Marijampolė

Noriu pažymėti, kad UAB “Seifneta” nuo 2007m. Birželio mėnesio naudoja „Free e-pay“ bankinių apmokėjimų pranešimų sistemą. 2009. Gruodžio mėnesį atnaujinome „Free e-pay“ sistemos versiją, su įdiegtais saugos elementais.

IT Projektų vadovas:
Tautvydas Papeika
t.papeika@seifneta.lt