KAUNO TECHNOLOGIJOS UNIVERSITETAS
INFORMATIKOS FAKULTETAS
KOMPIUTERIŲ KATEDRA

Albinas Grigaliūnas

SIP signalinių pranešimų, naudojant Asterisk serverį, saugumo užtikrinimo tyrimas

Magistro darbas

Darbo vadovas
doc. Tomas Adomkus

Kaunas, 2010

KAUNO TECHNOLOGIJOS UNIVERSITETAS
INFORMATIKOS FAKULTETAS
KOMPIUTERIŲ KATEDRA

Albinas Grigaliūnas

SIP signalinių pranešimų, naudojant Asterisk serverį, saugumo užtikrinimo tyrimas

Magistro darbas

Recenzentas
Rimantas Plėštys
2010-05-31

Vadovas
doc. T. Adomkus
2010-05-31

Atliko
IFN8/3 gr. Stud.
Abinas Grigaliūnas
2010-05-31

Kaunas, 2010

Turinys

1. ĮVADAS

Telekomunikacijų pasaulyje sparčiai plėtojantis naujoms technologijoms atsiranda naujos tarpusavio bendravimui skirtos priemonės. Jei ankščiau žmonės vieni kitus šaukte šaukdavo, vėliau atsirado laidiniai bei mobilieji telefonai, tai šiuo metu vis populiaresnis tampa balso perdavimas interneto tinklais. Žinant, kad pats paprasčiausias tokios paslaugos įdiegimas nereikalauja įrengti jokios specialios techninės įrangos ir, kad yra akivaizdus ekonominis naudingumas, ši paslauga tampa dar populiaresnė. Potencialus VoIP panaudojimas yra gerokai platesnis nei galimybė pasikalbėti su užjūrio draugu nemokant nė cento vietiniam telekomui.

Tikriausiai nereikia nei minėti, kad informacija šiais laikais yra viena brangiausių prekių. Norint užtikrinti saugų balso perdavimą pirmiausiai reikia užtikrinti šios balso sesijos saugumą. Neužtikrinus sesijos sudarymo saugumo galiniai vartotojai gali netekti ne tik balso perdavimo paslaugų, bet susidurti su konfidencialios informacijos paviešinimu ar net finansiniais nuostoliais.

Kaip ir tradicinėje analoginėje telefonijoje, taip ir dabartinėje VoIP technologijoje - pokalbio, konferencijos ar vaizdo sesijai sudaryti reikalinga signalizacija. IP telefonijoje sesijai sudaryti ir kontroliuoti dažniausiai naudojami H.323 ir SIP protokolai, kurių pagalba duomenų paketai yra nukreipiami tarp pokalbį sudariusių abonentų. Kadangi SIP protokolas yra ganėtinai naujas lyginant jį su H.323 protokolu, todėl nuspręsta plačiau susipažinti su šiuo protokolu ir jo saugumo užtikrinimo ypatybėmis.

SIP signaliniai pranešimai yra neatsiejama VoIP paslaugų dalis, todėl šių pranešimų saugumui turėtų būti skirtas toks pats dėmesys koks yra skiriamas IP telefonijai. Šie sesijos sudarymo pranešimai yra siunčiami tais pačiais nesaugiais interneto tinklais, ne gana to jie siunčiami kaip paprastas atviras tekstas. Nuolat didėjant kibernetinių nusikaltėlių skaičiui būtina nedelsiant susirūpinti SIP pranešimų saugumu. Užtikrinti signalinių pranešimų saugą VoIP paslaugų tiekėjams tikrai sudėtingas uždavinys, grėsmių sąrašai, kylantys naudojant SIP protokolą, yra gana nemaži, tačiau yra sukurta nemažai apsaugos priemonių, protokolų ir mechanizmų norint apsisaugoti nuo potencialių pažeidėjų.

Šiame darbe bus nagrinėjami SIP signalinių pranešimų saugos užtikrinimo mechanizmai, apimantys ne tik vartotojų galinę įrangą, bet ir tarnybinių stočių apsaugą. Nagrinėjamos temos aktualumą pabrėžia daugybė išleistų knygų apie SIP protokolą, taip pat parašyta daug straipsnių apie sesijos sudarymo saugumą. Pradedant kalbėti apie šio protokolo saugumo užtikrinimą, reikėtų susipažinti su pagrindiniais SIP tinklą sudarančiais komponentais, perduodamų užklausų bei atsakymų struktūra, bei pagrindinėmis grėsmėmis kylančiomis seanso sudarymo metu. Autoriaus Travis Russell knygoje „Session Initiation

Protocol (SIP) controling convergent networks“ apžvelgiami visi SIP tinklą sudarantys elementai, išanalizuota SIP protokolo struktūra, naudojami pranešimų tipai, registracijos ir valdymo ypatumai. Taip pat išanalizuotos saugumo atakos prieš šį tinklą, palyginamos saugumo užtikrinimo priemonės, bei pateikiami sprendimai kaip apsisaugoti nuo šių atakų. Tai yra nauja knyga išleista McGraw – Hill kompanijos 2008 metais, kuria remiantis analitinėje darbo dalyje bus apžvelgti SIP tinklą sudarantys komponentai, taip pat pagrindinės SIP protokolo savybės ir kylančios grėsmės. Saugumo užtikrinimui autorius siūlo naudoti griežtą SIP pranešimų maršruto parinkimą, pranešimų šifravimą, slaptažodžius ir kreipties valdymą, autentifikavimą ir autorizavimą. Šioje knygoje nėra pateikta konkrečių priemonių, kaip šifravimo algoritmai ar autentifikavimą ir autorizavimą užtikrinančios priemonės, todėl gilesnei SIP protokolo saugumo analizei jos nenaudosime [1].

Kaip ir pirmoje nagrinėtoje knygoje, taip ir H. Sinnreich ir A. B. Johnston knygoje „Internet Communications Using SIP“, visų pirma, aptariama SIP tinklo ir SIP protokolo struktūra ir savybės. Knygoje aptariamas DNS ir ENUM panaudojimas SIP protokolui ir su tuo susijusios grėsmės. Autoriai taip pat analizuoja užkardų ir tinklo adresų transliavimo funkcijų, bei su šia funkcija susijusių protokolų STUN, TURN ir ICE, panaudojimą SIP paslaugų realizavimui ir saugumo užtikrinimui. Ši knyga bus naudinga darbui, nes be jau minėtų apsaugos būdų analizuojami kiti įvairūs apsaugos būdai. Autoriai aprašo daugybę mechanizmų, kurie užtikrintų konfidencialumą, integralumą ir autentiškumą. Siūloma naudoti MD5 santraukos algoritmą slaptažodžiams, kad jie būtų siunčiami ne atviru tekstu, taip pat TLS protokolą, kuris leistų patikrinti vartotojų sertifikatus, šifravimą IP lygmenyje panaudojant IPsec protokolą, saugų SIP protokolą SIPS. Nors SRTP protokolas yra naudojamas ne signaliniams pranešimams perduoti, o pačiam balso duomenų srautui, knygoje šie du dalykai susiejami kadangi SIP protokolas gali pasitarnauti sesijos raktų perdavime. Ši knyga mano darbui bus aktuali, nes joje aptariama daugybė SIP protokolo saugumo mechanizmų [2]. S. Kašėtos ir T.Adomkaus knygoje „Telefonijos informacijos ir VoIP sauga“ taip pat trumpai aptariamos SIP protokolo saugumui kylančios grėsmės taip pat aprašomi SIP saugos mechanizmai, kurių veikimas pateikiamas iliustruotose pavyzdžiuose. Tai yra mokomoji knyga, kurioje pateikta susisteminta informacija apie SIP saugumą, joje pateikti SIP protokolo mechanizmai yra tinkami, tačiau išanalizuoti nepakankamai giliai. Ši knyga darbe bus panaudota analitinėje dalyje supažindinant su SIP protokolui kylančiomis grėsmėmis [3].

Rumunijos telekomunikacijų ir informatikos universiteto studentų straipsnyje „Evalution of Security and Countermeasures of a SIP based VoIP Architecture“ aprašomos konkrečios Asterisk serverio ir galinių SIP įrenginių atakos: paslaugų neteikimas UDP

užliejimo atakomis (SIP telefonų ir Asterisk serverių užliejimas INVITE žinutėmis, sesijos nutraukimas užliejant BYE žinutėmis, registracijos ištrinimas ir pagrobimas). Apsaugai nuo šių atakų siūloma naudoti užkardas bei įsilaužimo aptikimo (IDS) sistemas. Straipsnyje pateikti SIP atakų antraščių pavyzdžiai ir pateikti apsaugos mechanizmai praktinėje darbo dalyje bus naudingi apsaugant Asterisk tarnybinę stotį [11].

Dar vienas SIP protokolo saugos mechanizmas aprašomas Matthew Stafford knygoje „Signaling and Switching for Packet Telephony“. Autorius siūlo naudoti raktų valdymo protokolą SDP. Taip pat šioje knygoje aprašomas SIP ir SS7 signalizavimo protokolų sąveika. Be abejo, labai svarbu užtikrinti signalizavimo pranešimų saugumą ir suderinti du skirtingus tinklus IP ir PSTN. Kadangi šiomis dienomis tai vis dar aktuali tema, todėl mano darbe bus aptartas saugumo užtikrinimas tarp šių dviejų skirtingų protokolų [9].

Thomas Porter knygoje „Practical VoIP security“ rašo, kad nesvarbu koks tinklas būtų H.323, SIP ar paremtas kitokiu protokolo panaudojimu, reikalauja naujo požiūrio į informacijos saugumą. Šioje knygoje aprašomas VoIP saugos planas apimantis tiek fizinę tinklo saugą, tiek SIP signalinių pranešimų saugą. Manau, kad darbe nagrinėjant SIP saugumo temą būtų galima aprašyti ir pateikti saugumo planą. Autorius taip pat išnagrinėjęs daugybę autentifikavimo būdų. Galima būtų paminėti PKI infrastruktūrą, sertifikatų ir MAC panaudojimą. Šioje knygoje aprašomas Asterisk serveris ir jo funkcijos, ši informacija bus reikalinga, kadangi mano darbe ši tarnybinė stotis veiks kaip SIP serveris [5]. Asterisk panaudojimas VoIP paslaugoms taip pat aprašomas Paul Mahler knygoje „VoIP Telephony with Asterisk“. Literatūros šaltiniuose kaip pats paprasčiausias VoIP paslaugų apsaugos būdas minimas numatytojo slaptažodžio tarnybinėse stotyse pakeitimas. Netgi pateikiami konkretūs pavyzdžiai, kaip panaudojus „gamyklinius“ slaptažodžius buvo įsilaužta į tūkstančius kompiuterinių sistemų ir nuskanavus atidarytus prievadus ar atidarius naujus, kurie galėjo būti panaudoti persiunčiant reikalingą duomenų srautą, bei atlikus tam tikrus konfigūravimo veiksmus, maršrutai buvo parduodami legalioms telefonijos kompanijoms mažesniais įkainiais. Buvo persiųsta milijonai telefoninių skambučių per taikomąsias tarnybines stotis, apmokestinant telefonines kompanijas už naudojimąsi tariamu tinklu ir susižeriant sau nemažą sumą pinigų. Tačiau slaptažodžiai yra tik pati pradžia yra daug daugiau priemonių kurių turi būti imtasi, kad būtų apsaugotas SIP tinklas. Šioje knygoje daugiau dėmesio yra skiriama Asterisk tarnybinės stoties diegimui ir konfigūravimui nei apsaugos mechanizmų taikymui. Informacija iš šios knygos bus naudinga atliekant praktinę magistrinio darbo dalį [4].

VoIP yra realaus laiko paslaugos, todėl vienas pagrindinių šių paslaugų parametrų yra paslaugos kokybės užtikrinimas (QoS). PSTN ir TDM PBX gynėjai ilgą laiką gąsdino

vartotojus VoIP QoS, kad nubaidytų vartotojus nuo VoIP paslaugų. Paslaugos kokybę galima būtų vertinti pagal tris kriterijus: klausymo arba girdėjimo kokybė, pokalbio kokybė ir tinklo kokybė. Kadangi SIP protokolas neužtikrina paslaugos kokybės ir yra naudojamas tik pokalbio ar vaizdo konferencijos sesijai sudaryti, o paslaugos kokybės užtikrinimą atlieka kiti protokolai, todėl šios temos darbe nenagrinėsime [7, 8].

Dar viena aktuali šio darbo tema yra kuriamo saugaus SIP tinklo modeliavimas ir imitavimas OPNET programine įranga. Šios programinės įrangos aktualumą pabrėžia daugybė išleistų straipsnių apie VoIP tinklo, tame tarpe ir SIP pranešimų, apsaugos mechanizmų modeliavimą, charakteristikų tyrimą. Larry L. Peterson ir Bruce S. Knygoje „Network Simulation Experiments Manual“ patiekiama VPN ir užkardų realizavimas OPNET modeliavimo programa ir pateikiami statistiniai rezultatai gauti imitavus apsaugoto tinklo darbą [6]. Straipsnyje „Teaching IP Encryption and Decryption Using The OPNET Modeling and Simulation Tool“ aprašomas IPsec protokolo realizavimas sudarant VPN tunelius OPNET modeliavimo programoje [12]. Naudojant OPNET programinę įrangą ištirsime galimus SIP signalinių pranešimų apsaugos būdus ir remiantis gautais tinklo simuliavimo rezultatais paanalizuosime saugaus SIP įtaką sesijos sudarymui.

Praktinėje darbo dalyje bus tiriamas SIP signalinių pranešimų pažeidžiamumas ir saugos priemonių panaudojimas šių pranešimų saugaus perdavimo užtikrinimui. Vietiniame tinkle bus įdiegtas Asterisk serveris, kuriame sukuriami ir sukonfigūruojami SIP vartotojai, taip pat sukonfigūruojamos darbo vietos su programiniais SIP telefonais. Darbe bus atliekamas SIP slaptažodžių atsparumas „BruteForce“ bei Žodyno atakoms, Asterisk serverio atsparumas SIP pranešimais paremtomis DOS atakomis. Darbe saugiam SIP pranešimų perdavimui bus naudojamas OpneVPN-AS. Prieš sukuriant realų veikiantį tinklą, naudojantis OPNET modeliavimo programa, bus sukurtas ir susimuliuotas virtualus tinklas su įvairiomis SIP pranešimų apsaugos priemonėmis.

Temos aktualumas kylant vis didesnėms grėsmėms iš viešojo interneto tinklo būtina užtikrinti perduodamos informacijos konfidencialumą, autentiškumą ir vientisumą, todėl sudarant balso sesiją ar naudojantis kitomis VoIP teikiamomis paslaugomis, pirmiausiai būtina užtikrinti VoIP sesijos signalinių pranešimų saugumą.

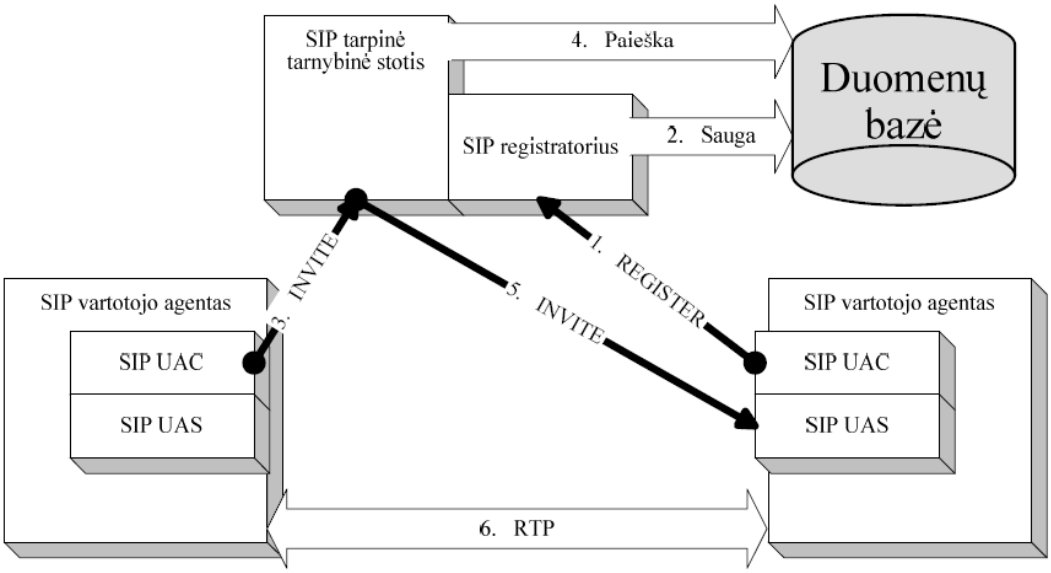
Magistrinio darbo tikslas SIP signalinių pranešimų, naudojant Asterisk serverį, saugumo užtikrinimo tyrimas.

Darbo uždaviniai:

1. Išanalizuoti VoIP saugumo problemas naudojant SIP protokolą.
2. Naudojant Opnet modeliavimo programą išanalizuoti SIP sesijų sudarymo trukmę, įdiegus saugos elementus.
3. Ištirti SIP signalinius pranešimus naudojant Asterisk serverį.
4. Pateikti išvadas ir pasiūlymus.

2. SIP PROTOKOLO STRUKTŪROS IR SAVYBIŲ ANALIZĖ

Prieš pradėdami analizuoti SIP protokolui kylančias grėsmes ir galimus apsisaugojimo nuo atakų būdus, reikėtų aptarti patį SIP protokolą bei SIP tinklą sudarančius pagrindinius elementus. Tipinė SIP tinklo schema ir SIP pranešimų kelias pateikiami 1 pav [3].



1 pav. Tipinė SIP tinklo schema ir SIP pranešimų kelias

Taigi, SIP (Sesijos inicijavimo protokolas) – taikomojo ir seanso lygmens signalizavimo protokolas, skirtas nustatyti, pakeisti ar užbaigti daugialypėms sesijoms, VoIP telefonijos sujungimams, skubių pranešimų siuntimui ir t.t. SIP sukuria ir valdo sesijas naudodamas tam tikrus pranešimų tipus arba metodus, kurie yra aprašyti RFC dokumentuose. SIP pranešimų sąrašas pateiktas 1 lentelėje.

1 Lentelė. SIP pranešimų sąrašas.

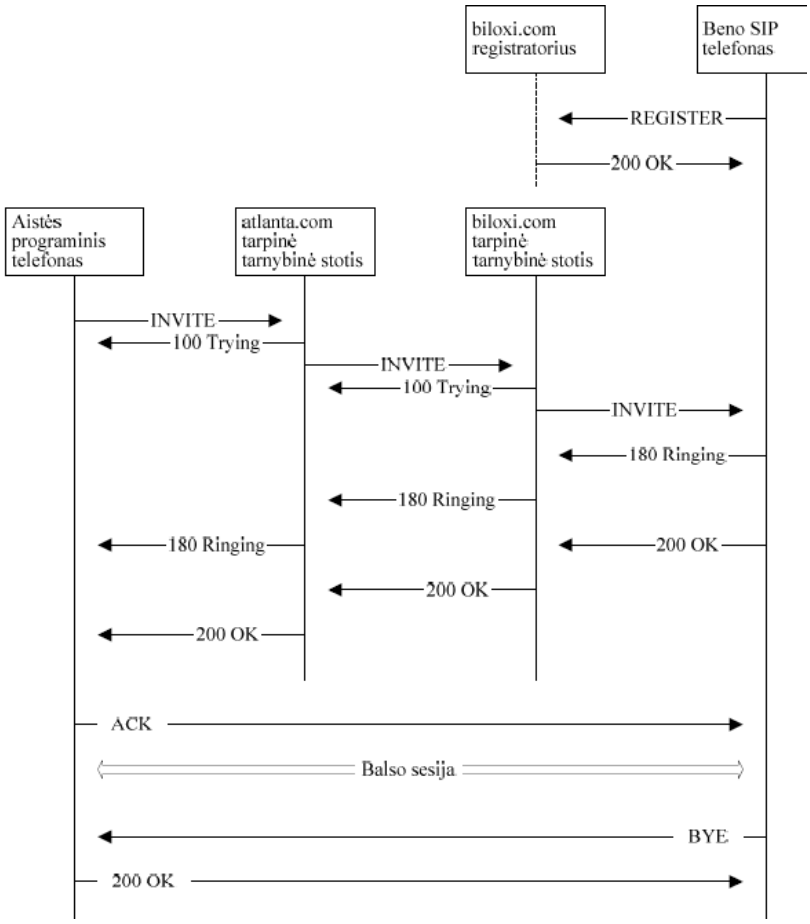
SIP pranešimas	Aprašymas
INVITE	Seanso inicijavimas
ACK	Galutinio atsakymo į INVITE patvirtinimas
BYE	Seanso pabaiga
CANCEL	Besitęsenčio seanso nutraukimas
REGISTER	Vartotojo URI registracija
OPTIONS	Įrangos galimybių ir nustatymų užklausa
INFO	Skambinimo signalizacijos tarpinės informacijos transportas
PRACK	Parengto atsakymo patvirtinimas
UPDATE	Seanso informacijos papildymas ar atnaujinimas
REFER.	Vartotojo peradresavimas pagal URI
SUBSCRIBE	Pranešimų apie įvykius registracija
NOTIFY	Pranešimų apie įvykius transportas
MESSAGE	Žinučių transportas
PUBLISH	Vartotojo aktyvumo informacijos atnaujinimas tarnybinėje stotyje

Pranešimų sąrašas nėra uždaras ir vis papildomas naujais pranešimais. Atsakymai į SIP pranešimus yra skaitmeniniai ir yra skirstomi į 6 klases pagal pirmąjį skaitmenį, kaip pateikta 2 lentelėje [3].

2 lentelė. Atsakymai į SIP pranešimus.

Klasė	Aprašymas
1xx	Informaciniai ir parengtiniai kodai. Užklausos vykdymas dar nebaigtas.
2xx	Sėkmingas įvykdymas. Užklausa įvykdyta.
3xx	Nukreipimas. Užklausą reikia pakartoti kitu adresu.
4xx	Kliento klaida. Užklausa neįvykdyta dėl klaidos užklausoje. Pataisius užklausą galima kartoti.
5xx	Tarnybinės stoties klaida. Užklausa neįvykdyta dėl adresato problemų. Galima pabandyti kreiptis į kitą adresatą.
6xx	Globali klaida. Užklausa nepavyko ir neturi būti kartojama.

Galima teigti, kad šis protokolas kilo iš paprasto pašto perdavimo (SMTP) ir hiperteksto perdavimo (HTTP) protokolų, todėl daugelis funkcijų aprašytų IETF standarto RFC 3261 dokumente taip pat kilo iš šių dviejų protokolų. 2 pav. pateikiamas SIP skambučio sekos pavyzdys.



2 pav. SIP skambučio seka

SIP protokolas buvo išvystytas, kad palaikytu penkis pagrindinius sesijos sudarymo ir išardymo elementus [1]:

- Sesijos dalyvių vieta;
- sesijos dalyvių pasiekiamumas (angl. availability);
- sesijos dalyvių galimybės (angl. capability);
- sesijos sąranka;
- sesijos valdymas.

Tam, kad pasiektų visas šias galimybes, SIP protokolui reikalingas tinklas, galintis aprūpinti specifinėmis funkcijomis. Taip pat reikalingos specifinės funkcijos vidinio tinklo objektams ir galinių vartotojų įrenginiams.

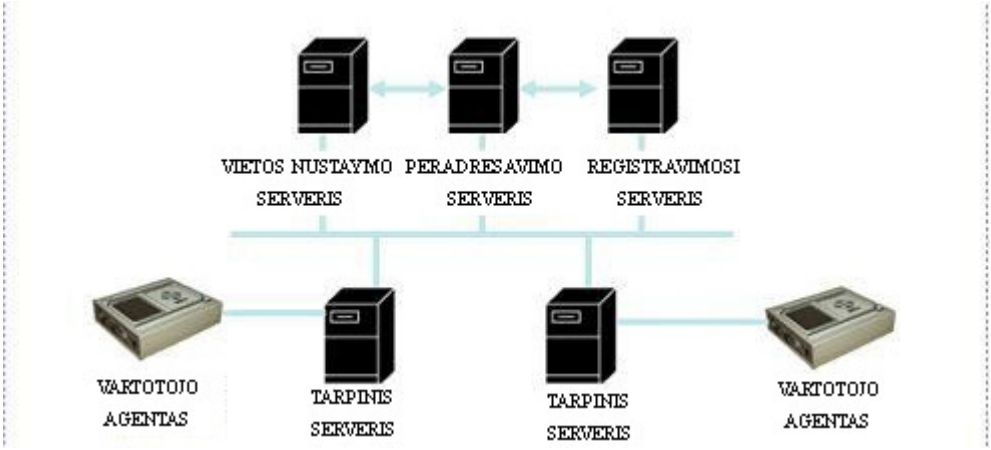
Sesijos dalyvių vieta gaunama vartotojams registruojantis į registravimosi tarnybinę stotį. Registravimosi procesas leidžia SIP sužinoti kiekvieno vartotojo IP adresą, kai tik tas klientas prisijungia prie tinklo.

Sesijos dalyvių pasiekiamumas yra daug daugiau nei žinojimas, kad kliento SIP įranga įjungta ar išjungta. Galbūt vartotojas pasirinkęs skambučių persiuntimą į balso paštą arba tik specifinių skambučių priėmimą. Taip pat klientas gali apsibrėžti kokio tipo skambučiai bus priimami tam tikru paros metu. Taikomosios tarnybinės stotys naudojamos saugoti informaciją apie vartotojo pasiekiamumą, bei pranešti kada klientas yra pasiekiamas.

Kiekvieno sesijos dalyvio galimybės nustatomos pagal tai, kokiu galiniu įrenginiu jis arba ji naudojasi. Pagal tai sprendžiama kokias galimybes turi klientas ir apie tai pranešama kitiems vartotojams.

SIP sistema sudaryta iš dviejų pagrindinių elementų: vartotojo agentų (angl. User agents - UA) ir tinklo serverių 3 pav.:

- Vartotojo agento klientas (UAC) - skirtas SIP užklausų formavimui;
- vartotojo agento serveris (UAS) - skirtas priimti SIP užklausas iš UAC ir grąžinti atsakymus vartotojui.



3 pav. SIP tinklo architektūra

Norint sudaryti pokalbio sesiją vartotojų agentai yra būtini, kitaip tariant, be jų būtų tas pats kaip skambinti nežinant kam skambini. Vartotojų agentais yra laikomi abu klientų

įrenginiai naudojami sesijai sudaryti. Priklausomai nuo to, kuris įrenginys naudojamas sesijai sudaryti ir kuris priima kvietimą dalyvauti sesijoje skiriami vartotojo agento klientas ir vartotojo agento serveris. Dažniausiai vartotojų agentai yra kompiuteris su įdiegta programine įranga, PDA, USB telefonai prisijungiantys prie kompiuterio, tačiau UA gali būti ir tinklų sąsaja jungianti paketinį duomenų perdavimo tinklą su PSTN.

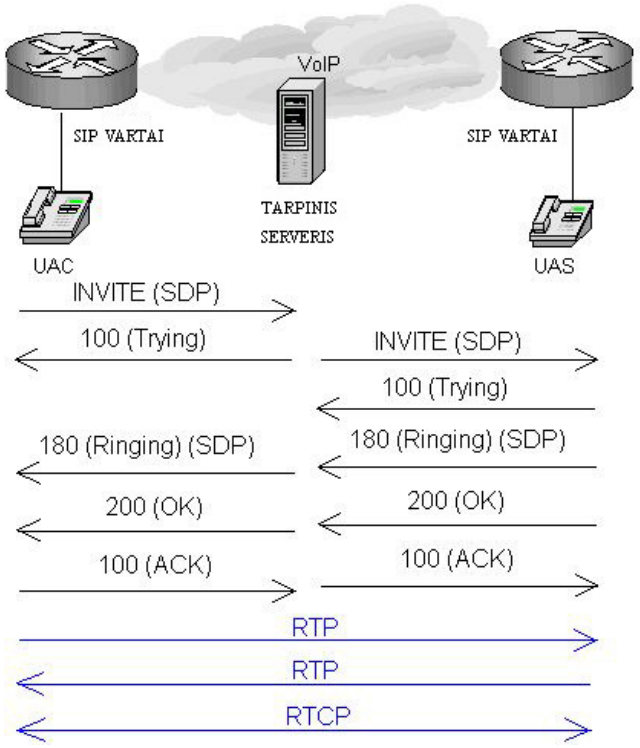
SIP serveriai naudojami IP adresų ir vartotojų vardų susiejimui, kad SIP užklausos, siunčiamos iš vieno vartotojo agento kitam būtų teisingai persiųstos. Vartotojų agentai registruojasi į SIP tarnybinę stotį pateikdami savo vartotojų vardus ir IP adresus, tokiu būdu yra nustatoma kliento buvimo vieta tinkle. Taip pat nustatomas vartotojo aktyvumas ir ar vartotojas priklauso tai pačiai sričiai, o gal būt naudojasi kitu SIP serveriu. Atsižvelgiant į skirtingas vartotojų užklausas, SIP tarnybinės stotys skirstomos į tris tipus [5]:

- Registravimosi serverius;
- tarpinius serverius;
- peradresuojančius serverius;

Registravimosi serveriai naudojami vartotojų įrenginių autentiškumo bei vietos nustatymui. Kai įrenginys yra įjungiamas arba pakeičia savo tinklo nustatymus (priskiriamas naujas IP adresas) siunčiama REGISTER žinutė į SIP tinklą, kad pateiktų naujus registracijos duomenis SIP tarnybinei stočiai.

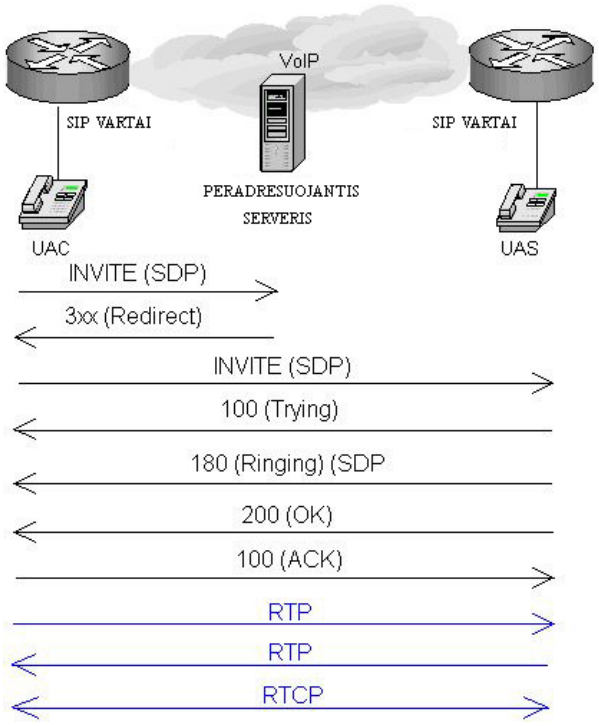
Registratorius gavęs naujus duomenis turi du pasirinkimus: priimti naują adresą ir išsaugoti jį vietos nustatymo serveryje arba atmesti pirmąją registraciją, taip priversdamas vartotoją atsiųsti autentifikavimo raktus, kad įsitikintų ar tai tas pats vartotojas. Antrasis pasirinkimas yra rekomenduojamas labiau bet kuriame SIP tinkle, nes padeda apsisaugoti nuo pačių paprasčiausių „man in the middle“ atakų. Jei autentiškumo nustatymas būtų registracijos proceso dalis, pašalintų daug sukčiavimo atvejų ir saugumo pažeidimų.

Tarpiniai serveriai yra įrenginiai naudojami persiųsti gautas užklausas atitinkamiems vartotojams 4 pav. Kad pasiektų reikiamą vartotoją užklausa gali būti persiųsta per keletą tarpinių serverių. Veikdamas kaip tarpinė tarnybinė stotis, SIP serveris gali teikti šias funkcijas: tinklo prieigos kontrolę, saugumo užtikrinimo, autentifikavimo ir prieigos suteikimo. Priklausomai nuo to kas siunčiama - užklausos ar atsakymai, tarpinė tarnybinė stotis gali veikti kaip klientas arba kaip serveris.



4 pav. Sesijos sudarymas naudojant tarpinį serverį

Priešingai nei tarpinis serveris, peradresuojantis serveris nepersiunčia užklausų kitiems serveriams. Šis serveris naudojamas alternatyvių adresų, vartotojų užklausoms, suteikimui. Tai atliekama dėl įvairių priežasčių, tokių kaip tarpinių serverių užimtumas arba tinklo srauto paskirstymas. Gavęs užklausą iš vartotojo kliento, peradresuojantis serveris siunčia 3xx atsakymą klientui, nurodydamas alternatyvų adresą galutinio vartotojo pasiekimui 5 pav.

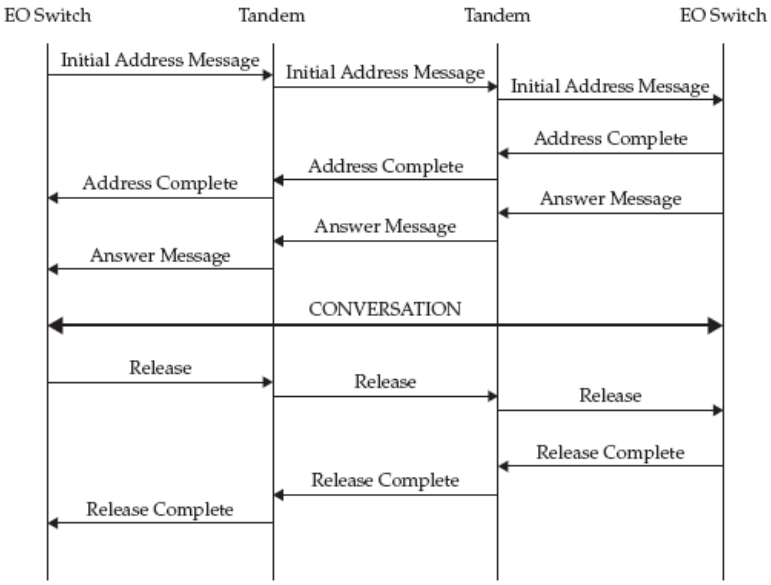


5 pav. Sesijos sudarymas naudojant peradresuojantį serverį

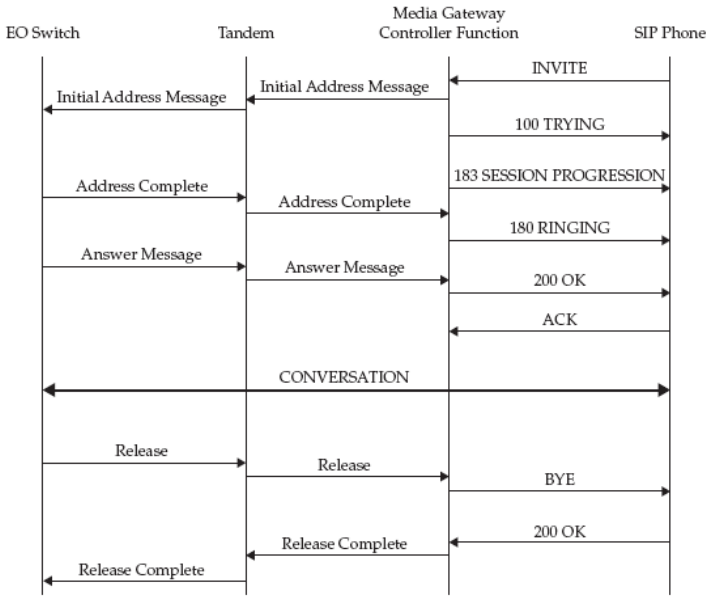
SIP signalizacijos protokolas yra nepriklausomas nuo transportinio protokolo ir gali būti naudojamas kartu su keletu šių protokolų: TCP, UDP, srauto kontrolės perdavimo protokolu SCTP. Taip pat šis protokolas suderinamas su abejomis interneto protokolo versijomis IPv4 ir IPv6.

2.1. Signalizacijos protokolų suderinamumas

Atsižvelgiant į tai, kad šiuo metu naudojama ne vien tik VoIP telefonija, būtina suderinti skirtingų technologijų signalinius pranešimus. Šiame skyriuje trumpai aptarsime VoIP telefonijos SIP signalinių pranešimų suderinamumą su tradicinės telefonijos SS7 signalizacija 6, 7 pav. Ši sąveika būtina vien dėl to, kad praeis nemažai laiko, kol visi vartotojai pereis prie IP telefonijos.



6 pav. Sesijos sudarymas naudojant SS7 signalizaciją



7 pav. SIP ir SS7 signalizacijų sąveika

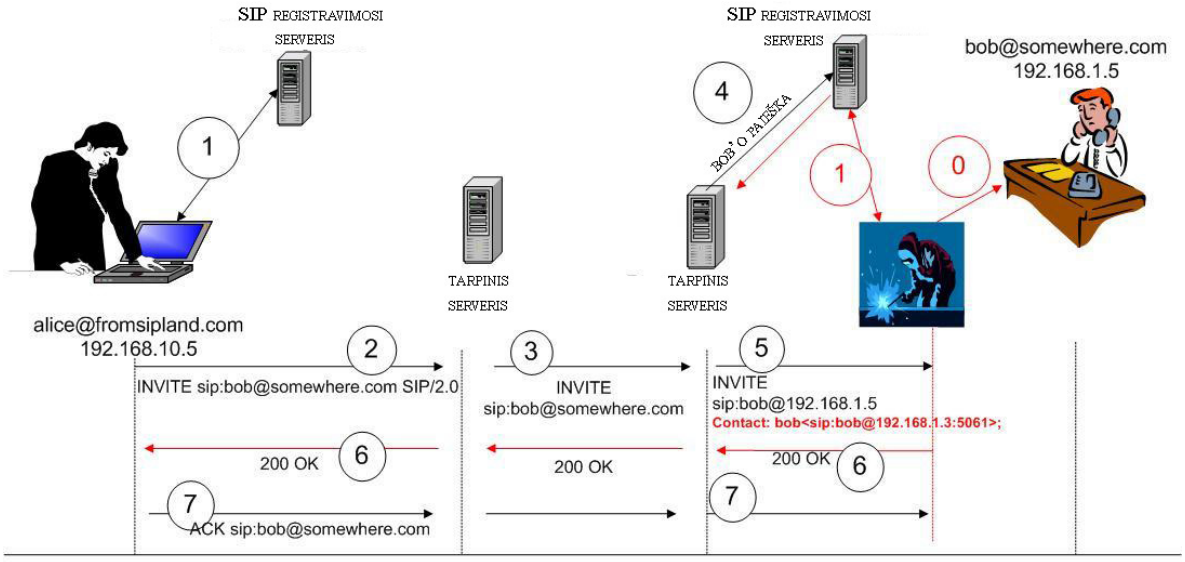
2.2. SIP protokolo pažeidžiamumas

Yra daugybė tinklo pažeidimo formų, tačiau šiame skyriuje išanalizuosime dažniausiai pasitaikančias VoIP tinklo atakas. Šiandieniniame interneto tinkle ypatingai paplitusios sukčiavimo ir paslaugų neteikimo (DoS) atakos, tačiau pažvelkime ir į kitus įvairius tinko pažeidimo tipus, paanalizuokime kaip jie veikia ir kokią žalą gali padaryti tinklo operatoriams bei vartotojams.

Pirmiausiai, reikėtų įsigilinti į tai kaip piktavalis prieina prie tinklo resursų, tai padėtų suprasti kaip atakos prasideda ir nuo ko reikėtų pradėti norint apsisaugoti nuo jų. Programišius ketindamas užpulti tinklą pradeda savo darbą nuo tinklų stebėjimo. Iš pradžių ieškoma tinklų su lengva prieiga, kuriuose palikti atidaryti prievadai su atitinkamais numeriais arba palikti numatytieji slaptažodžiai. Išanalizavus tokią sistemą ir radus pažeidžiamą vietą, duomenys apie spragas įrašomi vėlesniems išpuoliams. Daugybė saugumo pažeidimų gali būti aptikta naudojant tinklo skenavimo įrankius, kurie naudojami tinklo sutrikimams šalinti, tačiau toks įrankis piktavalio rankose gali pridaryti daug žalos.

2.2.1. Registracijos pagrobimas

SIP protokolas sesijos sudarymui naudoja atviro teksto žinutes, tai reiškia, kad kiekvienas asmuo turintis kompiuterį ir šiokių tokių programavimo žinių, gali slapta prisijungti prie tinklo ir įrašinėti SIP pranešimus. Išanalizavęs šiuos pranešimus piktavalis gali išgauti legalaus vartotojo jautrią informaciją – privatų ar viešą tapatumą 8 pav. Vėliau panaudojęs šią informaciją asmuo gali gauti prieigą prie operatoriaus tinklo ir panaudoti ją savo reikmėms.



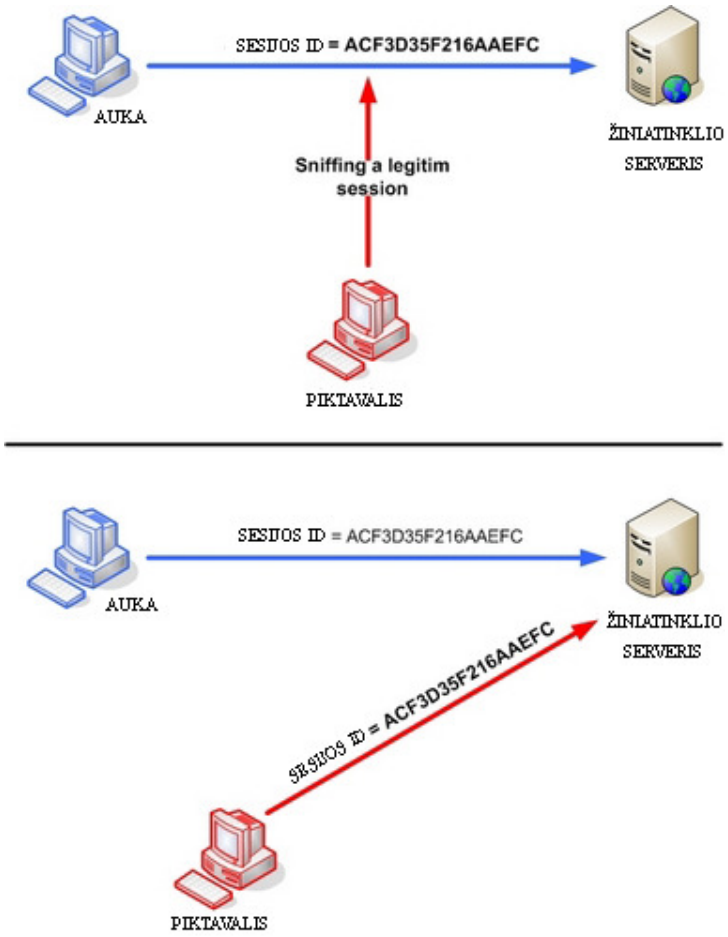
8 pav. Registracijos pagrobimas

Tarkime, kad vartotojas užsiregistravo tinkle, jo buvimo vieta įrašoma į registravimosi tarnybinę stotį. Visos užklausos, elektroninis paštas, trumposios žinutės yra siunčiamos į šią

vietą. Programišius gauna prieigą prie to paties tinklo ir panaudoja tą pačią legalaus vartotojo informaciją, gautą išanalizavus to vartotojo siunčiamus SIP pranešimus, tam, kad užsiregistruotų tinkle. Teisėto vartotojo registracija lieka nepakeista, todėl registracijos serveriui atrodo, kad šis klientas tik pakeitė vietą tinkle, kurią nurodė prisiregistravęs piktavalis. Kitas būdas naudojamas registracijos užgrobimui – teisėto vartotojo registracijos žinučių pagrobimas ir persiuntimas panaudojant naują registravimosi vietą [1, 23].

2.2.2 Sesijos užgrobimas

Sesijos užgrobimas vykdomas panašiai kaip ir registracijos užgrobimas, tačiau ši ataka panaudojama kitaip. Sesijos užgrobimas vykdomas sesijos eigoje ir yra kilęs iš žiniatinklio. Tam, kad palengvintų pastovų autentiškumo nustatymą, voratinklio (angl. web) kūrėjai įvedė „slapukų“ sąvoką. Slapukas yra ne kas kitas kaip duomenų failas, paprastai susidedantis iš sesijos tapatybės (angl. sesion ID). Perėmus ir nukopijavus šiuos slapukus, piktavaliui suteikiama pilna prieiga prie jau vykstančios sesijos 9 pav. Tai reiškia, kad sesijos metu programišius turi prieigą prie visų jūsų transakcijų ir vartotojo informacijos. Dauguma svetainių sugeneruoja slapukus, naudodamos algoritmą, kuris unikalaus identifikatoriaus sukūrimui naudoja laiko žymą ir IP adresą. Šis sesijos autentifikavimo būdas sukelia daug saugumo pažeidimų, todėl nėra rekomenduojamas naudoti SIP tinkle.



9 pav. sesijos užgrobimas [24]

Sesijos pagrobimo tikrinimui naudojamas laiko ir datos žymų tikrinimas siunčiamose užklausose bei gaunamose atsakymuose. Šios žymos turi būti palygintos su vidinio laikrodžio reikšme, jei gautas skirtumas yra didesnis nei 30 minučių, tikėtina, kad sesija buvo užgrobta. Slapuko galiojimas baigiasi pasibaigus sesijai [1].

2.2.3 Apsimetinėjimo atakos

Jei dažnai naudojatės internetu, tikriausiai esate susidūrę su tokio tipo atakomis. Yra daugybė svetainių atrodančių lygiai kaip originalūs tų svetainių puslapiai, tačiau programišių sukurti analogiški puslapiai naudojami pavogti informaciją iš patiklių lankytojų. Dažniausiai tokių atakų taikiniai yra bankų ar atsiskaitymo kreditinėmis kortelėmis internetiniai puslapiai.

Tarpinės tarnybinės stotys nukreipia vartotojus ne į tikras, o į programišių sukurtas svetaines, kur prašoma suvesti identifikavimo kodus, slaptažodžius ar kitą jautrią informaciją. Kitas tokios atakos pavyzdys, kuris buvo panaudotas ir Lietuvoje, elektroninio laiško siuntimas bankinės sistemos naudotojui. Tokio laiško turinyje nurodoma, kad dėl techninių kliūčių reikia atnaujinti vartotojo duomenis ir pateikiama nuoroda į suklastotą svetainę.

Taip pat yra galimybė kompromituoti DNS serverį, tokios atakos dar vadinamos DNS nuodijimu. Tokios atakos metu „nulaužiamas“ DNS serveris ir pakeičiamas atitinkamų tarnybinių stočių IP adresas. Tokios atakos tikėtinos ir SIP tinkle, kuriame DNS naudojamas IP adresų susiejimui su domenais ir jų taikomosiomis programomis.

Tokių atakų žala SIP tinkle būtų tokia pati kaip visose kitose sistemose. Klientų peradresavimas per sukčių taikomąsias tarnybines stotis sukeltų rimtų padarinių tiek klientui tiek paslaugos tiekėjui [1, 2].

2.2.4 Pranešimo turinio modifikavimas

Kaip jau minėjau ankščiau, SIP pranešimai perduodami atviru tekstu, todėl piktavaliui perėmusiam šiuos pranešimus nereikia turėti dešifratoriaus, kad perskaitytų kas juose parašyta. Šios atakos metu susiduriama ne tik su konfidencialumo, bet ir su duomenų vientisumo pažeidimu.

Įsivaizduokite, kad programišius perėmęs INVITE užklausą, pakeistų jos FROM antraštę įrašydamas savo adresą. Tai suteiktų piktavaliui prieigą prie tinklo, kuriuo jis nėra įgaliotas naudotis taip pat leistų sudaryti sesijas su kitais legaliais klientais apsimetant kažkuo kitu. Rūpestį kelia ir SIP pranešimų siuntimas, kadangi šie pranešimai taipogi siunčiami atviru tekstu, piktavalis gali ne tik perskaityti konfidencialią informaciją, bet ir visiškai pakeisti pranešimo tekstą [1]. Apsisaugojimui nuo šių atakų naudojamas pranešimų šifravimas, kurį išnagrinėsime tolimesniuose skyriuose.

2.2.5 IP telefonijos šiukšlės

IP telefonijos šiukšles būtų galima išskirti į:

- Pranešimų siuntimu pagrįstos šiukšlės panašios į elektroninio pašto šiukšles. Šio tipo šiukšlės realizuojamos naudojant VoIP telefonijos signalizavimo protokolus, tokius kaip SIP;
- skambučiais pagrįstos šiukšlės – apgaulingi skambučiai arba prekyba skambinant telefonu.

Šiukšlių siuntimas plėtojosi taip pat greitai, kaip ir priemonių prieš jas kūrimas. Kai tik išleidžiama kokia nors atsakomoji priemonė prieš šiukšlinimą, šiukšlintajai bando pakeisti savo žinutes taip, kad šios apeitų atsakomąją priemonę. Aptikti IP telefonijos šiukšles yra žymiai sunkiau nei elektroninio pašto šiukšles, o smulkūs VoIP operatoriai nesiima jokių prevencijos priemonių kol ši problema rimtai neiškilo [13].

2.3. SIP saugumo užtikrinimas

Saugumas IP telefonijoje apima ne tik visas tradicinės telefonijos saugumo problemas, bet ir prideda visas duomenų tinklo saugumo problemas. Operacinėms sistemos, kuriuose įdiegta IP-PBX įranga gresia tos pačios atakos, kurios sutrikdo kitas tarnybines stotis.

VoIP saugos užtikrinimas turėtų prasidėti nuo saugos politikos sukūrimo, kuri turėtų apimti:

- Fizinį saugumą;
- loginį balso ir duomenų atskyrimą;
- telefono įrenginius;
- duomenų šifravimą.

Saugumo politikoje taip pat turėtų būti skirtas dėmesys signalizacijos protokolų saugumui. Pagrindiniai SIP tinklo saugumo aspektai [2]:

- Autentiškumo nustatymas;
- prieigos suteikimas;
- konfidencialumas;
- vientisumas;
- privatumas;
- nepaneigiamumas (non-repudiation).

Šiuo metu SIP protokolas palaiko penkis saugumo mechanizmus:

- TLS;
- HTTP santrauka;
- IPSec su IKE;
- IPSec be IKE;
- S/MIME.

2.4. SIP sauga naudojant Asterisk serverį

Asterisk – atvirojo kodo telefonijos variklis ir įrankių rinkinys, įgalinantis kūrėjus ir integratorius kurti pažangias komunikavimo sistemas visiškai veltui. Asterisk galima įdiegti į šias operacines sistemas [14]:

- Linux;
- Mac OS X;
- FreeBSD;
- OpenBSD;
- Sun Soliaris.

Taip pat jis palaiko daugybę protokolų tokių kaip: H.323, SIP, MGCP, SCCP. Panaudojant IAX protokolą Asterisk sujungia balso ir duomenų perdavimą per skirtingų tipų tinklus. Asterisk gali būti panaudotas kaip [4]:

- Privati telefoninė stotis (PBX);
- balso pašto tarnyba;
- konferencinių skambučių tarnybinė stotis;
- IP telefonijos tarnybinė stotis;
- skambučių ir faksogramų šifravimui;
- skirtingų tinklų sąsaja su IP telefonija.

Šiuo metu galima pasirinkti vieną iš trijų Astrerisk tarnybinių stočių versijų, kurios skiriasi vartotojo sąsaja ir funkcinėmis galimybėmis:

- Asterisk;
- Asterisknow;
- Asterisk bussines;

Pirmas svarbus žingsnis prieš diegiant telefoninę sistemą – tinkamai pasirinkti reikiamą versiją. Sekantis ne ką mažiau svarbus žingsnis – tarnybinės stoties techninės įrangos pasirinkimas. Iš dalies tai paprastas, bet kartu ir komplikuotas žingsnis: paprastas dėl tos priežasties, kad bet kuri x86 paremta sistema yra tinkama, tačiau patikimas sistemos darbas priklausys nuo to, kaip bus suprojektuota platforma. Renkantis techninę įrangą reikia visapusiškai įvertinti būsimą projektą, įvertinant koks sistemos funkcionalumas turės būti palaikytas. Nuo to priklausys procesoriaus, pagrindinės plokštės bei maitinimo šaltinio pasirinkimas. Kita, papildoma techninė, įranga pasirenkama priklausomai nuo to su kokiomis skirtingomis technologijomis Asterisk serveris bus derinamas [10].

Nagrinėjant telefonijos sistemą reikėtų aptarti ir prietaisus, kuriuos ši sistema galų gale sujungia – telefonus. Būtų galima išskirti šias pagrindines galinių įrenginių rūšis:

- Fiziniai telefonai (analoginiai, skaitmeniniai, IP telefonai);

- programiniai telefonai;
- telefonijos sietuvai;
- terminalai.

Sukurta daugybė priemonių, skirtų kompiuterinių tinklų peržiūrai ir analizei. Pasinaudoję šiomis priemonėmis piktavaliai gali lengvai aptikti SIP kompiuterius bei nagrinėdami jų siunčiamą duomenų srautą išgauti naudojamus slaptažodžius. Todėl yra būtina nedelsiant imtis Asterisk tarnybinės stoties apsaugos priemonių nuo peržiūros atakų. Be abejo, yra sukurta daugybė metodų ir apsaugos įrankių – tereikia juos pritaikyti. Yra septyni paprasti žingsniai, kuriuos pritaikius SIP sesijos, naudojant Asterisk serverį, taps saugesnės [15]:

- Nepriimti SIP autentiškumo nustatymo prašymų iš visų IP adresų. Reikia nustatyti „permit=“ ir „deny=“ parametrus SIP konfigūracijos byloje sip.conf ir leisti tik „protingam“ poaibiui IP adresų pasiekti kiekvieną įrašytą vartotoją į sip.conf bylą;
- SIP konfigūracijos byloje sip.conf nustatyti parametrą “alwaysauthreject=yes”. Pagal nutylėjimą šio parametro reikšmė yra „no“, nustačius reikšmę „yes“ bus atmesti blogi autentiškumo nustatymo prašymai su galiojančiais bei negaliojančiais vartotojų vardais;
- SIP objektui naudoti stiprius slaptažodžius. Tai vienas svarbesnių žingsnių, kuris turėtų būti žengtas. Slaptažodžiui sudaryti turėtų būti panaudota mažiausiai 12 simbolių iš mažųjų ir didžiųjų raidžių, skaičių bei įvairių simbolių;
- blokuoti savo AMI tvarkyklės prievadus. Panaudojant parametrus „permit“ ir „deny“ manager.conf byloje leidžiant įeinančius ryšius tik iš žinomų kompiuterių, bei panaudoti stiprius slaptažodžius;
- kur galima, per SIP objektą, leisti tik vieną arba du skambučius tuo pat metu;
- padaryti SIP vartotojo vardus skirtingus nei jų plėtiniai;
- užtikrinti, kad numatytasis kontekstas yra saugus. Uždrauskite vartotojams, kuriems nenustatytas autentiškumas vykdyti mokamus skambučius. Arba visiškai uždrausti skambinti tiems vartotojams, kuriems nenustatytas autentiškumas nustatant parametrą „allowguest=no“ bendroje sip.conf bylos dalyje.

-

2.5. Išvados

- Atlikus SIP protokolo analizę, pateikiami pagrindiniai: SIP tinklą sudarantys komponentai, SIP pranešimai ir atsakymai į juos, taip pat SIP sesijos sudarymo pavyzdžiai.
- Atlikus literatūros analizę išryškėjo pagrindinės SIP sesijos sudarymo saugumo problemos, bei galimi apsisaugojimo būdai nuo šių saugumo spragų.
- Atlikus Asterisk serverio analizę išanalizuota kuriuose operacinėse sistemose gali būti įdiegtas šis serveris, pagrindinės šio serverio paslaugos bei išleistos versijos.
- Kaip parodė literatūros šaltinių analizė SIP saugos užtikrinimui neužtenka vien tik Asterisk serverio teisingos konfigūracijos apsisaugant nuo SIP sesijos sudarymo grėsmių. Reikalingi papildomi saugos mechanizmai užkertantys kelią įvairioms paslaugų neteikimo, registracijos ar sesijos užgrobimo, bei kitoms atakoms susijusiomis su šiuo protokolo panaudojimu.

3. PROJEKTUOJAMO SIP TINKLO STRUKTŪROS MODELIS

Saugaus SIP tinklo projektavimas, kaip ir bet kurios kitos sistemos projektavimas turėtų prasidėti nuo saugumo politikos sukūrimo, kuri turėtų apibrėžti kas turėtų būti apsaugota ir kokie yra apribojimai. Tam, kad saugumo politika būtų lankstesnė ir butų patogiau ja naudotis, ją galėtų sudaryti ne vienas, o keletas dokumentų apibrėžiančių skirtingų funkcinių dalių saugumą.

Praktinėje darbo dalyje bus atliekamas SIP protokolo saugumo tyrimas panaudojant Asterisk serverį. Saugumo užtikrinimui bus analizuojamas Asterisk tarnybinės stoties konfigūravimas bei OpenVPN panaudojimas SIP pranešimų perdavimui. Praktinį darbą būtų galima suskirstyti į šias dalis:

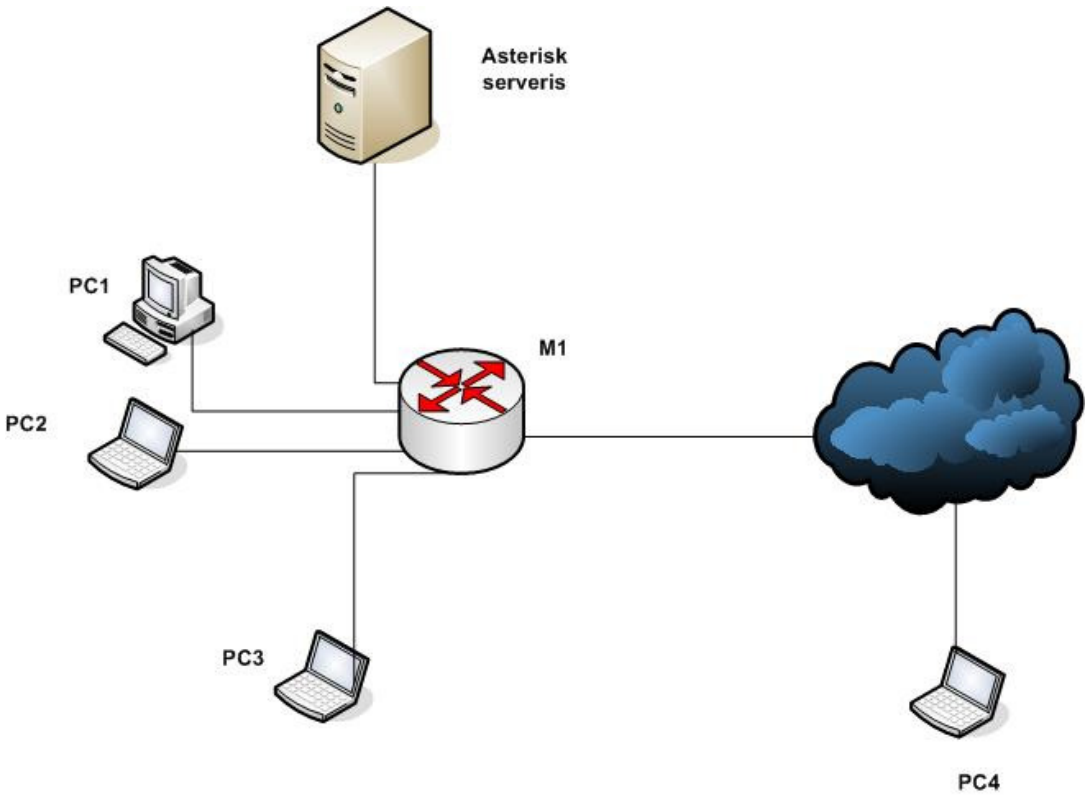
- asterisk serverio diegimas ir konfigūravimas;
- OpenVPN diegimas ir konfigūravimas;
- SIP saugumo ir kokybės parametrų tyrimas.

Tačiau prieš pradedant darbus reikėtų išanalizuoti būsimojo tinklo struktūrą, atsižvelgiant į reikiamą funkcionalumą apžvelgti techninę bei programinę įrangą. Projektinėje darbo dalyje bus analizuojama:

- SIP tinklo struktūra;
- Asterisk tarnybinių stočių versijos;
- SIP programiniai telefonai;
- Opnet modeliavimo programos rezultatai;

3.1. SIP tinklo struktūra ir saugumo analizė

Analizuojamas SIP tinklas, kurio struktūrinė schema pateikta 10 paveiksle, sudarytas iš trijų vietiniame tinkle esančių kompiuterių kuriuose įdiegti SIP programiniai telefonai, kompiuterio su įdiegta Asterisk tarnybine stotimi, maršrutizatoriaus, kuris kartu yra ir kartotuvas turintis 4 LAN prievadus ir bevielio ryšio galimybę, bei vieno nutolusio kompiuterio su SIP programiniu telefonu.



10 pav. Analizuojamo SIP tinklo modelio struktūrinė schema

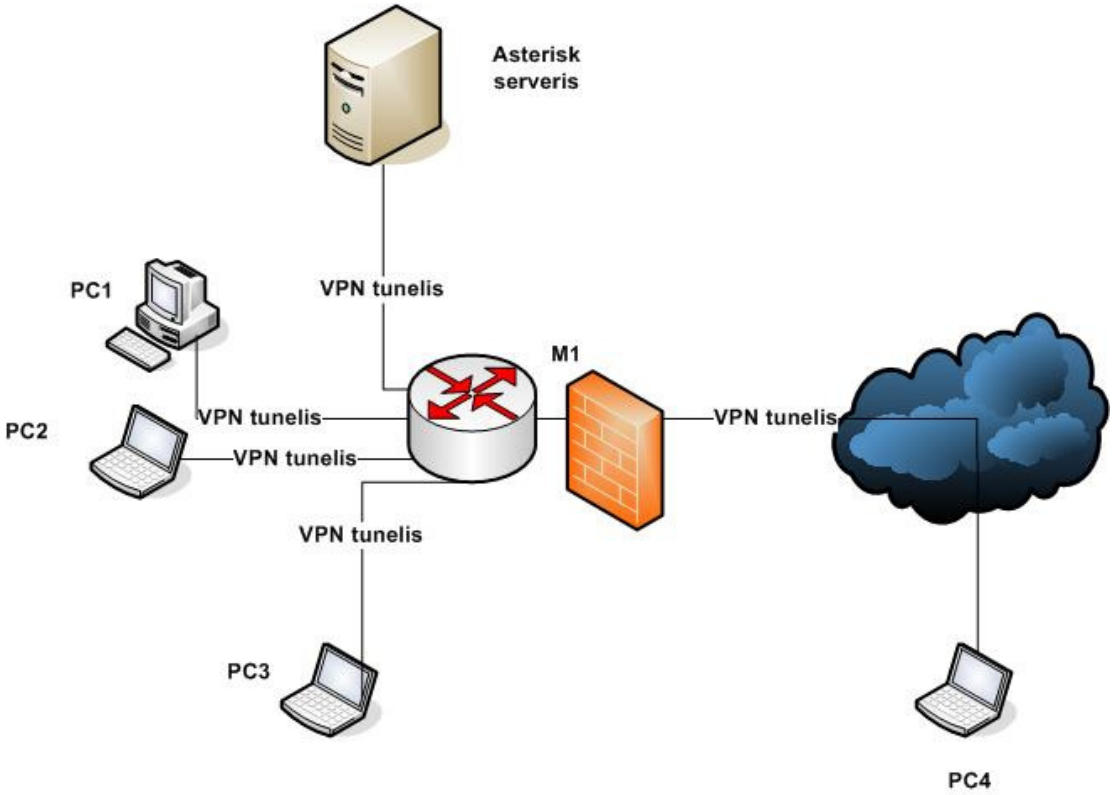
Vietiniame tinkle naudojami C klasės IP adresai (3 lentelė). Viena darbo vieta – PC4 yra nutolusi. LAN tinkle naudojami DNS adresai:

- Pageidautinas 84.32.84.6
- Alternatyvus 84.32.84.2

3 lentelė. LAN tinklo IP adresacija

Įrenginys	IP adresas	Potinklo kaukė	Tinklų sąsaja
Asterisk	192.168.1.100	255.255.255.0	192.168.1.1
PC1	192.168.1.101		
PC2	192.168.1.102		
PC3	192.168.1.103		
PC4	88.216.1.181	255.255.255.0	88.216.1.254
R1_VID	192.168.1.1	255.255.255.0	192.168.1.1
R1_IŠ	88.216.20.49	255.255.255.0	88.216.20.254

Kiekvienoje darbo vietoje įdiegtos antivirusinės programos, Asterisk tarnybinė stotis papildomai apsaugota panaudojant užkardą. SIP signaliniai pranešimai apsaugomi panaudojant VPN tunelius. Analizuojamo tinklo schema su įdiegtais saugos sprendimais pateikta 11 pav.



11 pav. Analizuojamo apsaugoto SIP tinklo modelio schema

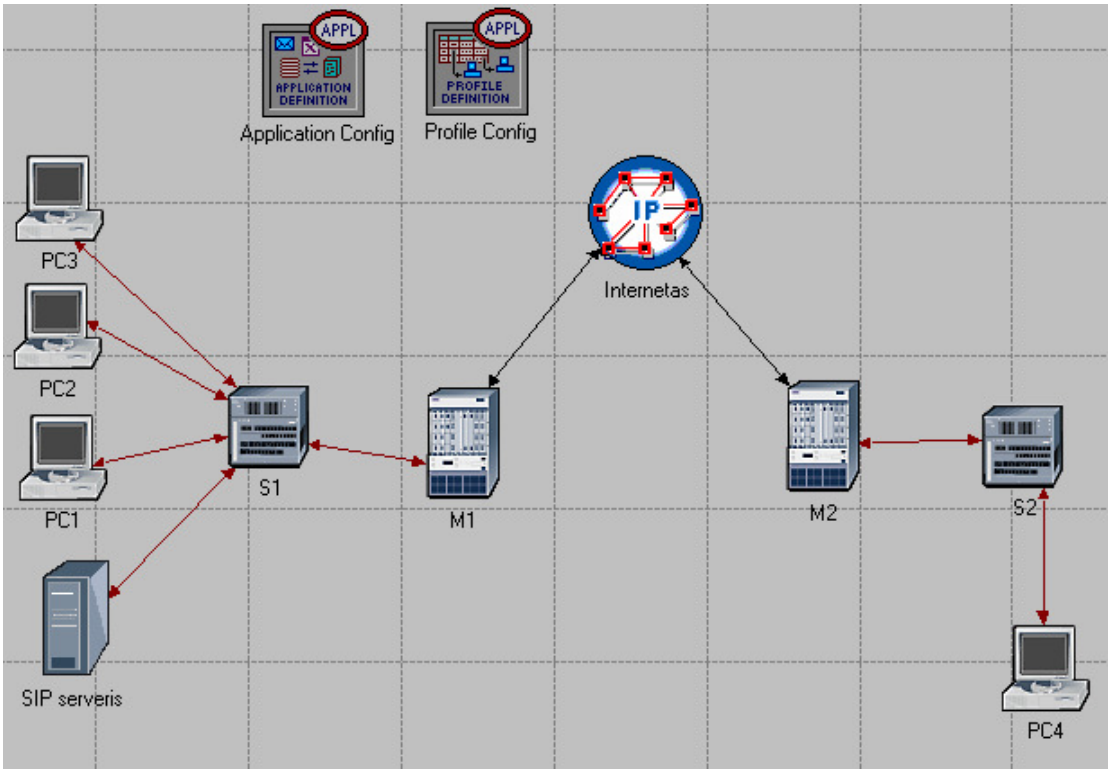
3.2. SIP tinklo simuliavimas OPNET modeliavimo programa

Kompiuterinių tinklų kūrimas reikalauja nemažų investicijų. Tam, kad tinklas būtų saugus ir patikimas reikia parinkti tinkamus nustatymus, topologiją bei tinkamus tinklo įrenginius. Tam, kad nešvaistyti pinigų įrangos pirkimui ir testavimui buvo pasiūlytas tinklų simuliavimo įrankis.

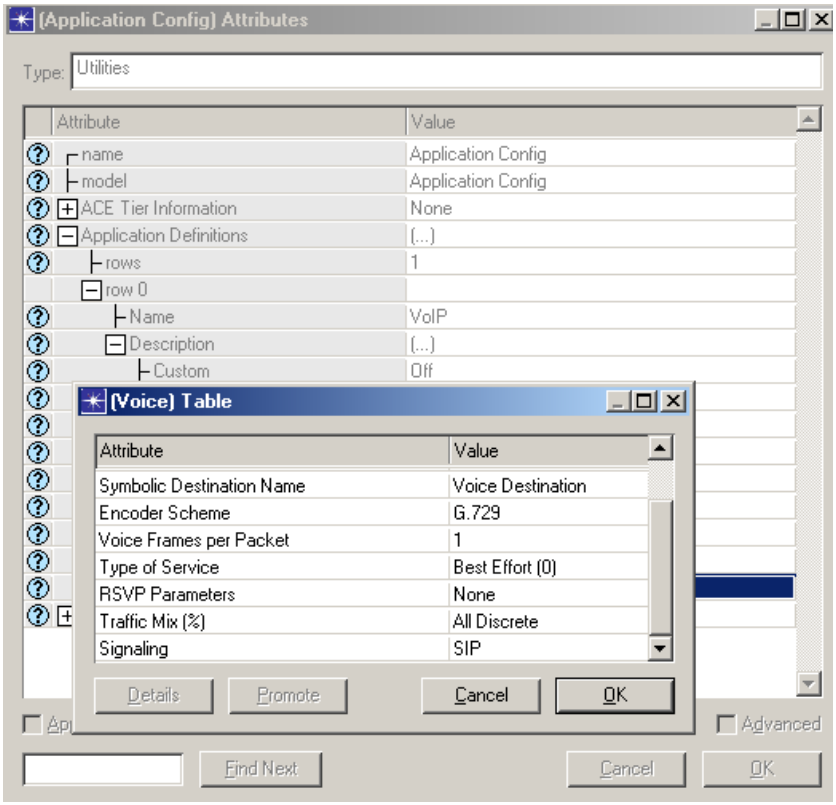
Sukuriamas scenarijus OPNET programoje turintis SIP tarnybinę stotį ir vartotojus naudojančius VoIP paslaugas su SIP signalizavimo protokolu 12 pav. Tinklo sukūrimui parenkame ir sukonfigūruojame šiuos objektus:

- Konfigūracijos blokai: Application Config, Profile Config.
- Darbo stotys: ethernet_wkstn.
- Komutatoriai: ethernet16_switch.
- Maršrutizatoriai: ethernet4_slip8_gtwy.
- Tarnybinės stotys: SIP_proxy_server.
- Sujungimai: 100BaseT, PPP_DS1 (dvikryptė)

Pirmiausiai aprašomos naudojamos paslaugos Application Config bloke, šiuo atveju pasirenkame realaus laiko VoIP paslaugas. Tam nustatome, kad bus naudojama viena paslauga - IP telephony ir signaling – SIP 13 pav.

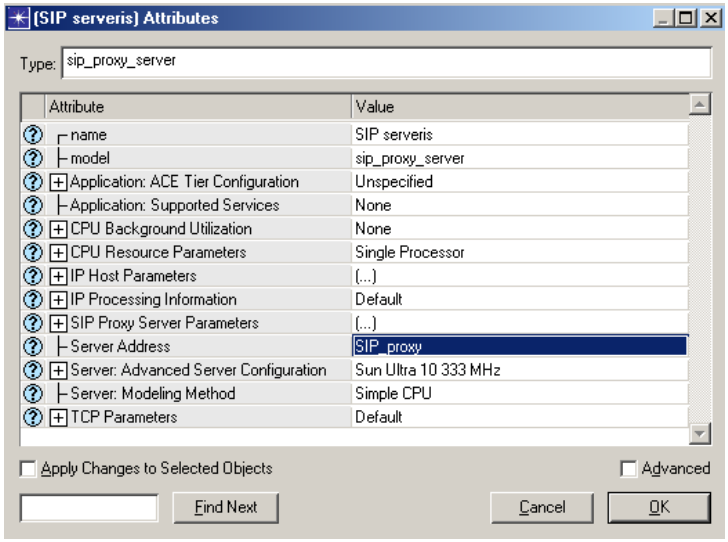


12 pav. Analizuojamo SIP tinko modelio schema OPNET modeliavimo programa



13 pav. VoIP paslaugų nustatymas

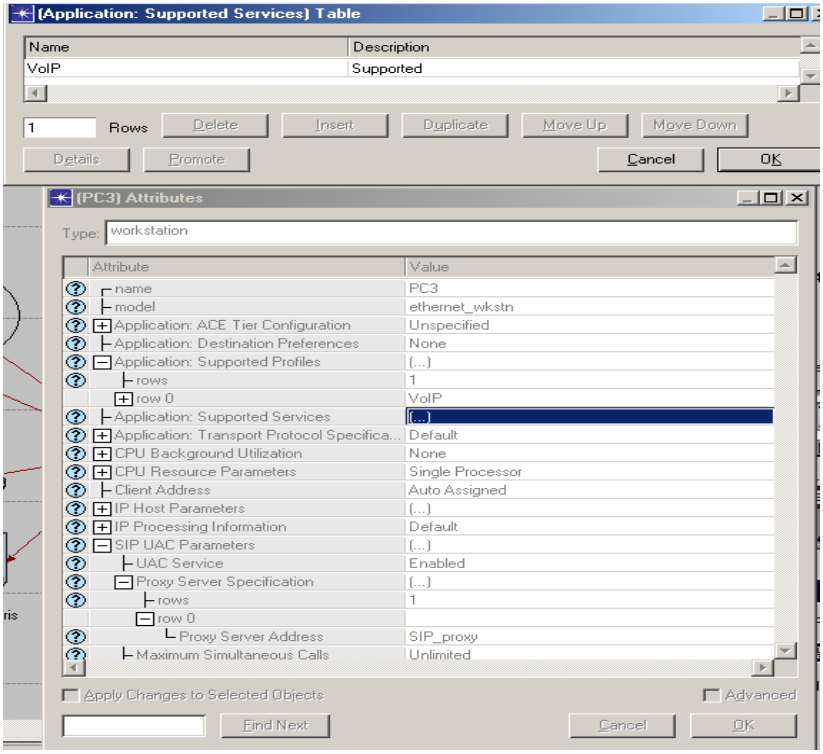
Toliau Profile Config bloke sukuriame vartotojų profilį VoIP paslaugoms, bei SIP proxy tarnybinėje stotyje nurodome serverio adresą – SIP_proxy 14 pav.



14 pav. SIP tarnybinės stoties konfigūravimas

Aprašius naudojamas paslaugas bei sukonfigūravus SIP tarnybinę stotį, atliekamas varototojų darbo vietų konfigūravimas VoIP paslaugoms su SIP signalizacija 15 pav. Atliekame šiuos nustatymų pakeitimus:

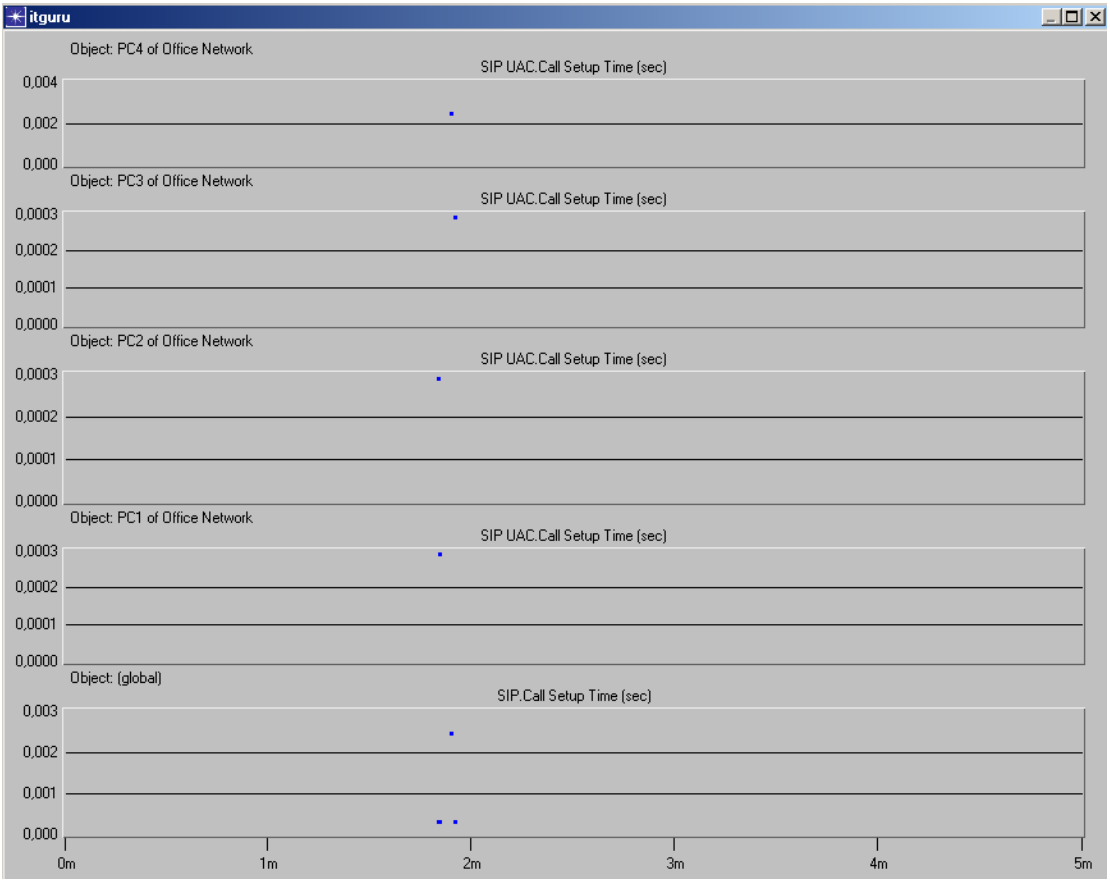
- Application supported profiles – VoIP.
- Application supported services –VoIP.
- UAC Service – Enabled.
- Proxy Server address – SIP_proxy.



15 pav. Darbo vietos konfigūravimas

Atlikus konfigūravimo darbus atliekamas tinklo simuliavimo procesas. Pasirenkami SIP sesijos sudarymo laiko rezultatai 16 pav. Kaip matyti iš gautos ataskaitos SIP pokalbiui

sudaryti, nenaudojant jokių apsaugos priemonių, vietiniame tinkle reikia 0,3 ms, o iš nutolusios darbo vietos – 2 ms.



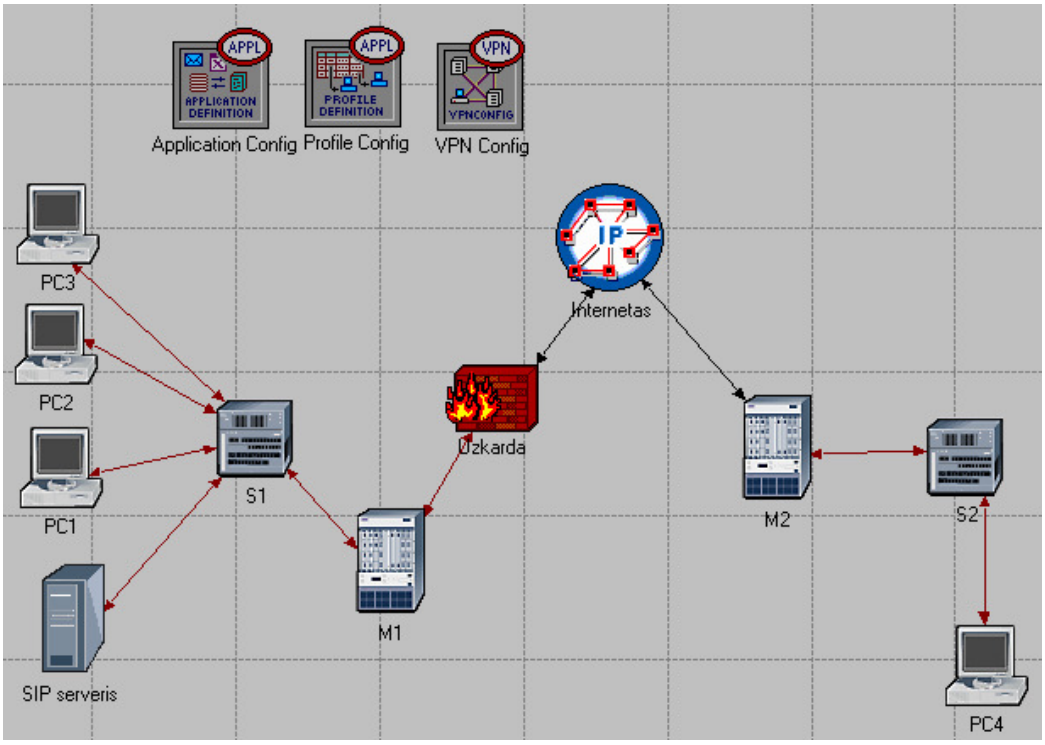
16 pav. SIP sesijos sudarymo laikas

Toliau papildome tinklą užkarda, kuri praleis tik VoIP srautą, ir VPN tuneliais, kurie naudojami vartotojų tapatybei nustatyti bei perduodamų duomenų šifravimui 17 pav. Šiuo atveju turimą tinklą papildome dviem elementais:

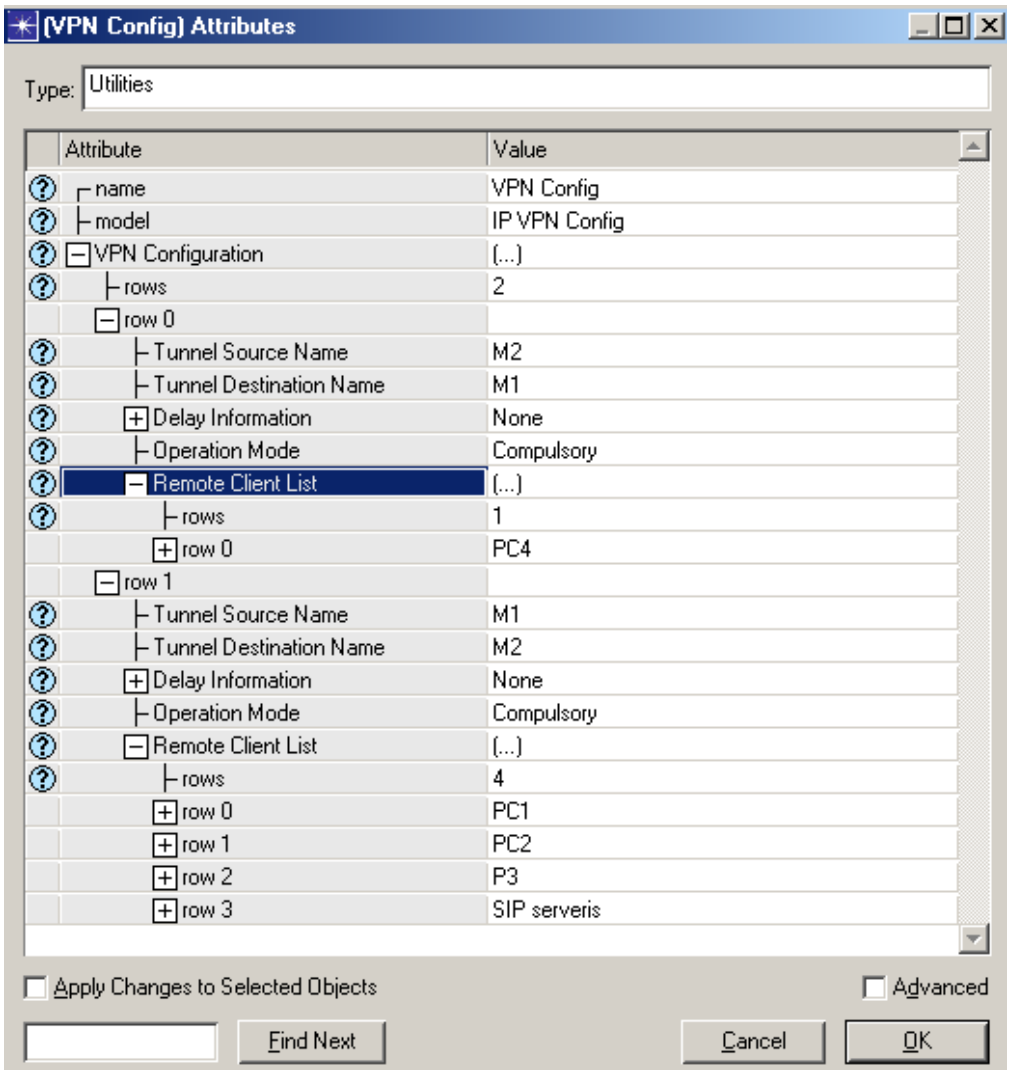
- Užkarda: Ethernet2_slip8_firewall.
- VPN: IP_VPN_Cnfig.

18 pav. Pateikiamas VPN serverio konfigūravimas, nustatomi tunelio pradinis ir galinis šaltiniai bei nutolusių klientų sąrašas.

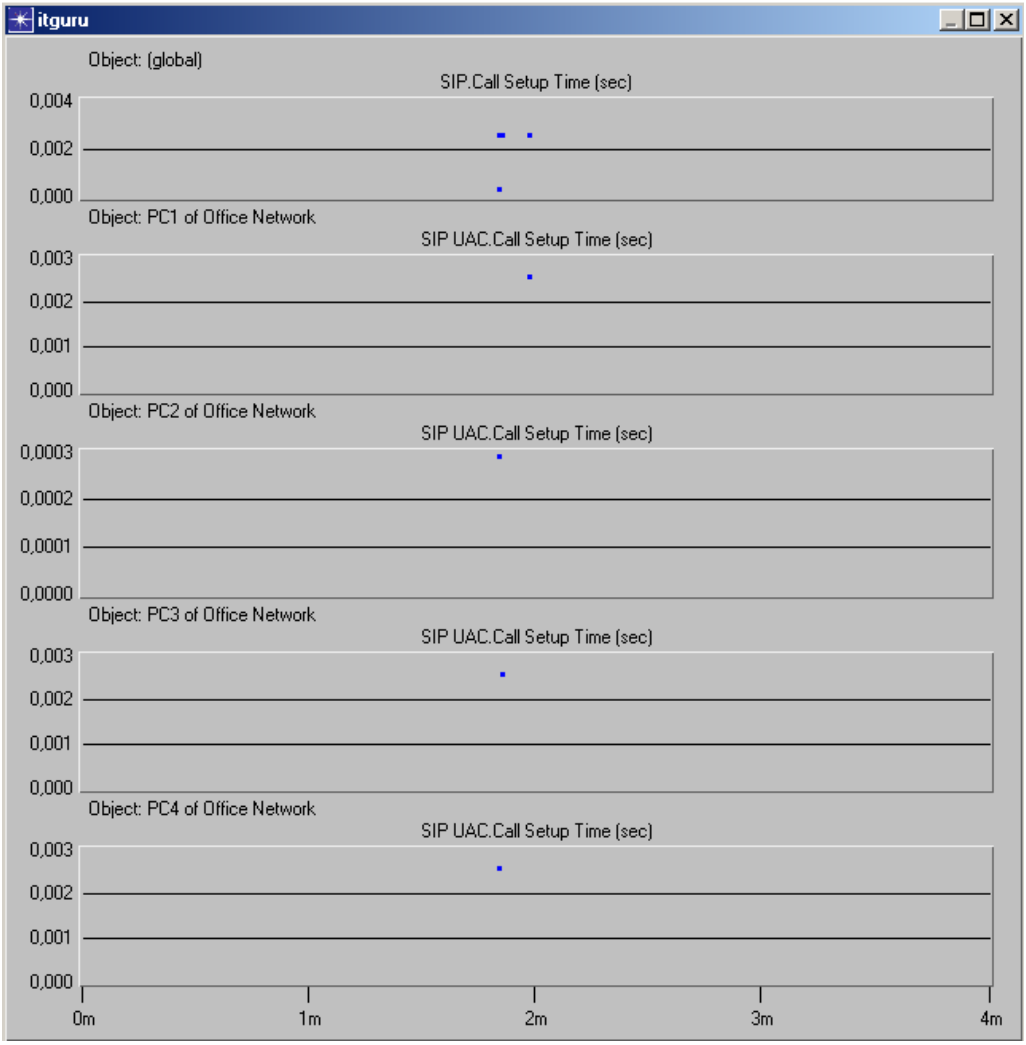
Kaip ir pirmuoju atveju, altikus konfigūravimo darbus paleidžiamas tinklo simuliavimo procesas. Gauta SIP sesijos sudarymo laikų ataskaita pateikiama 19 pav. Sulyginus apsaugoto SIP tinklo sesijos sudarymo laikus galima teigti, kad užkarda ir duomenų šifravimas SIP sesijos sudarymo laikui įtakos neturi.



17 pav. Analizuojamo SIP tinklo modelio schema OPNET modeliavimo programa



18 pav. VPN konfigūravimas



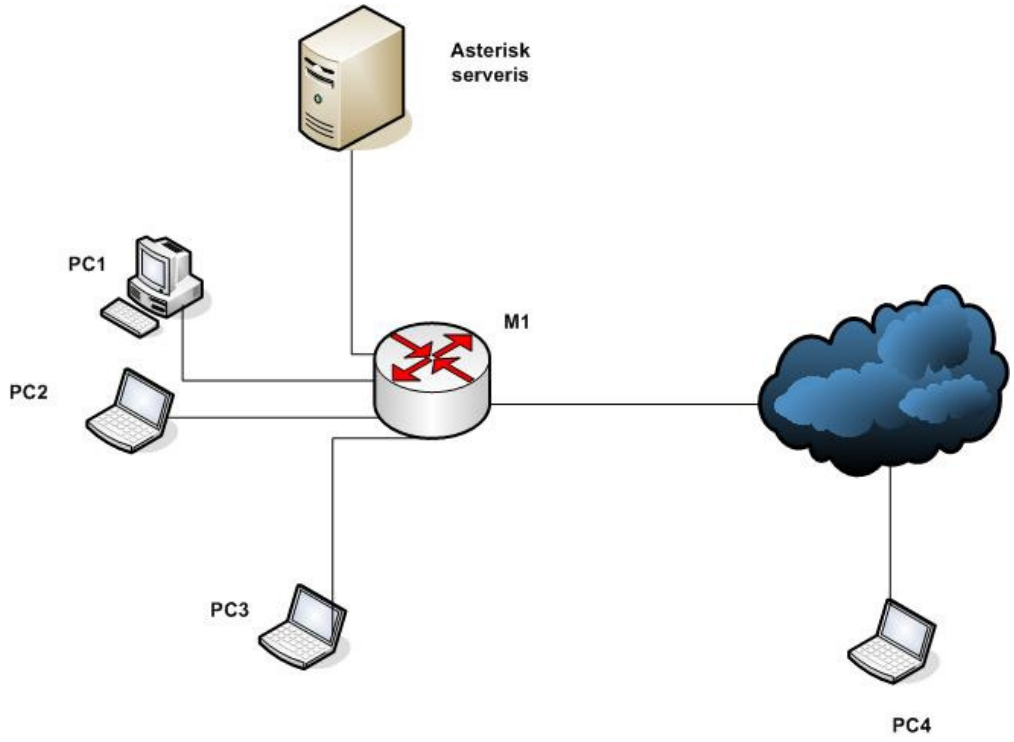
19 pav. SIP sesijos sudarymo laikas apsaugotame tinkle

3.3. Išvados

- Projektuojamame SIP tinklo modelyje, panaudojus OPNET modeliavimo programą, išanalizuotas neapsaugoto ir apsaugoto SIP tinklo sesijos sudarymo laikai.
- Sukurtas SIP tinklo modelis parodė, kad neapsaugoto ir apsaugoto SIP tinklo sesijos sudarymo laikai yra artimi 2 ms, todėl saugumo mechanizmų įdiegimas SIP sesijos sudarymo kokybei nepakenkia.
- Ribota OPNET modeliavimo programos akademinė versija neleido detaliau panagrinėti SIP sesijos sudarymo pranešimų saugos savybių. Taip pat dėl ribotos programos versijos nebuvo galima analizuoti SIP tinklo susidedančio iš didesnio vartotojų skaičiaus.
- Parenkant Asterisk serverio techninius parametrus tokius kaip atminties dydis, procesoriaus taktinis dažnis bei apkrova, turi būti atsižvelgta į šiuos parametrus: vartotojų skaičių, skambučio kokybę, skambinimo trukmę, saugumą, laiką nuo numerio surinkimo iki skambučio pradžios.

4. EKSPERIMENTINIO MODELIO REALIZACIJA

Praktinėje darbo dalyje analizuojamas SIP protokolo saugumo užtikrinimas naudojant asterisk serverį. Tyrimui atlikti sukonfigūruojamas vietinis tinklas, kurio struktūrinė schema pateikta 20 paveiksle, sudarytas iš trijų vietiniame tinkle esančių kompiuterių kuriuose įdiegti SIP programiniai telefonai, kompiuterio su įdiegtu Asterisk serveriu, maršrutizatoriaus, kuris kartu yra ir kartotuvas turintis 4 LAN prievadus ir bevielio ryšio galimybę, bei vieno nutolusio kompiuterio su SIP programiniu telefonu.



20 pav. SIP tinklo struktūrinė schema

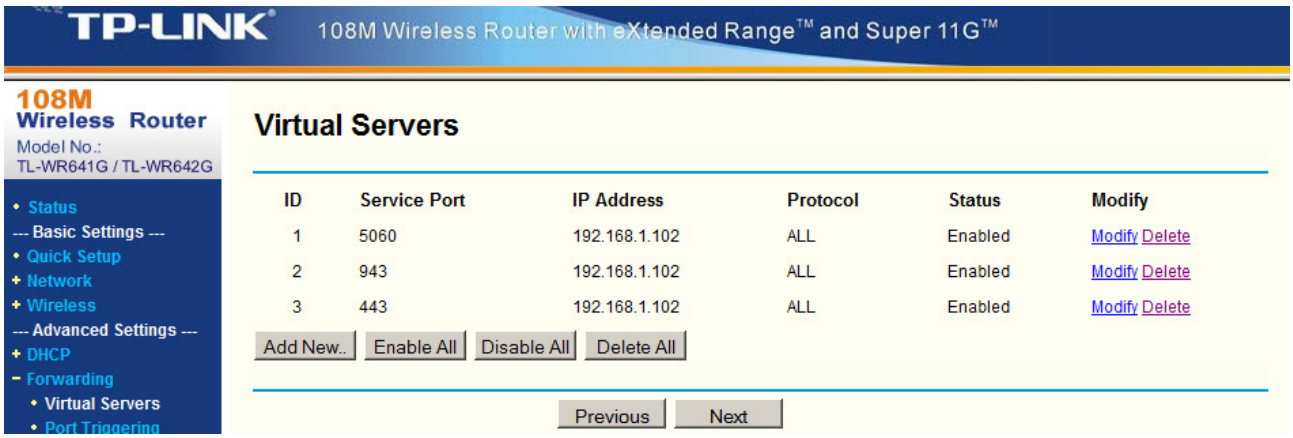
Vietiniame tinkle naudojama C klasės IP adresai, viena darbo vieta yra nutolusi. Maršrutizatoriuje veikia DHCP paslauga skirstanti IP adresus vartotojams 192.168.1.101 – 192.168.1.201 adresų ribose. Visi vietinio tinklo darbo vietų nustatymai pateikti 4 lentelėje. Tinkle naudojami DNS adresai:

- 84.32.84.6
- 84.32.84.2

4 lentelė. Vietinio tinklo nustatymai

Įrenginys	IP adresas	Potinklo kaukė	Tinklų sąsaja
Asterisk	192.168.1.102	255.255.255.0	192.168.1.1
PC1	192.168.1.110		
PC2	192.168.1.111		
PC3	192.168.1.103		
PC4	88.216.1.181	255.255.255.0	88.216.1.254
R1_VID	192.168.1.1	255.255.255.0	192.168.1.1
R1_IŠ	88.216.20.49	255.255.255.0	88.216.20.254

Tam, kad nutolusios darbo vietos vartotojas galėtų prisijungti prie Asterisk serverio maršrutizatoriuje nurodoma, kad visi prašymai jungtis 5060 prievado numeriu būtų nukreipiami į vietinio tinklo 192.168.1.102 IP adresą t.y. į asterisk tarnybinę stotį 21 pav. Kadangi tinkle veikia DHCP paslauga asterisk serverio IP adresas yra rezervuotas, priskiriamas pagal tinklo plokštės MAC adresą.



21 pav. Maršrutizatoriaus konfigūravimas

Darbo vietose įdiegtos Microsoft Windows operacinės sistemos, kurių versijos pateikiamos 5 lentelėje, taip pat naudojamos biuro programos, elektroninio pašto klientai bei programiniai SIP telefonai. Saugumui padidinti kiekvienoje darbo vietoje įdiegtos antivirusinės programos, bei įrankiai skirti aptikti ir pašalinti nepageidaujamą programinę įrangą. Kompiuteryje, kuriame įdiegtas Asterisk 1.6.2 versijos serveris, įdiegta Linux Centos OS 5.4 distribucija bei OpenVPN-AS (Access server) serveris. Tinklu perduodamiems duomenų paketams stebėti įdiegtas WireShark tinklo paketų analizatorius.

5 lentelė. Operacinių sistemų versijos

Įrenginys	Operacinė sistema	Atnaujinimo versija
PC1	MS Vista Home Premium	SP2
PC2	MS XP professional	SP3
PC3	MS XP professional	SP3
PC4	MS Windows 7 ultimate	

Kompiuteris PC4 veikia kaip piktavalis, jame įdiegta Cain&Abel programinė įranga skirta šniukštinėti tinklą, „nulaužinėti“ šifruotus slaptažodžius naudojant žodynines ir brutualios jėgos atakas.

Vietinio tinklo apsaugai perimetru, maršrutizatoriuje įdiegta užkarda. Šios užkardos paskirtis apsaugoti Asterisk serverį nuo DoS atakų:

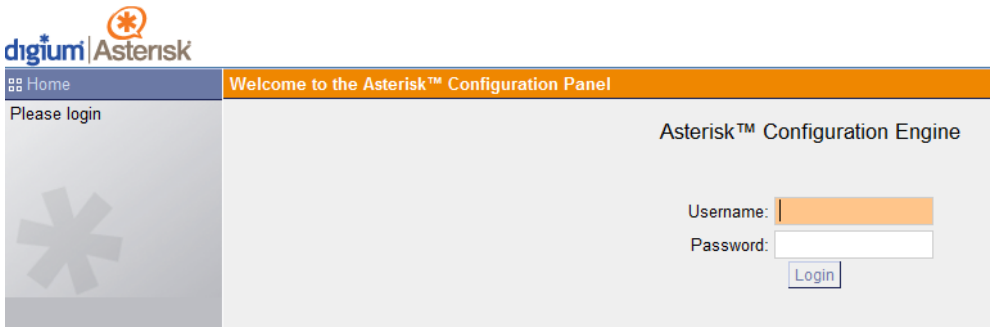
- ICMP užtvindymo;
- TCP – SYN užtvindymo;

- UDP užtvindymo.

4.1. Asterisk serverio įdiegimas ir klientų konfigūravimas

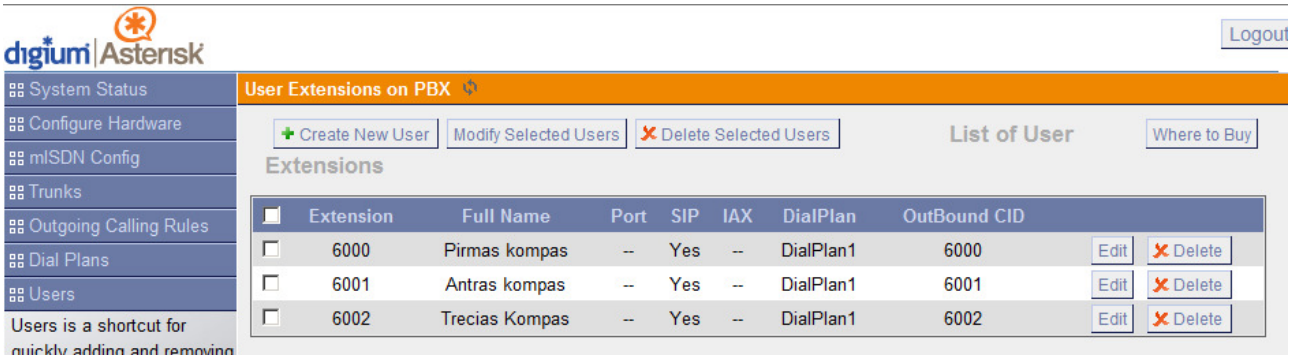
Parsiunčiame ir įdiegiame naujausią Asterisk serverio versiją (Asterisk 1.6.2) iš oficialaus asterisk.org tinklapio. Kad butų paprasčiau administruoti serverį įdiegiama grafinė sąsaja 22 pav.

Įdiegus grafinę administravimo sąsają pirmas svarbus žingsnis saugumo link yra standartinio vartotojo vardo ir slaptažodžio pakeitimas. Standartiniai vartotojų vardai tokie kaip: „admin“, „administrator“ ar „root“ turėtų būti pakeisti į jūsų sugalvotą, tačiau nebūtų susiję su įmonės pavadinimu, veiklos sritimi ir t.t., kurioje įdiegtas serveris. Taip bus apsunkintas vartotojo vardo atspėjimas žodyno ar kitokių atakų atveju. Administratoriaus slaptažodį turėtų sudaryti ne mažiau kaip 6 simboliai ir turėtų būti sudarytas iš didžiųjų, mažųjų raidžių, skaitmenų bei specialiųjų simbolių.



22 pav. Grafinė konfigūravimo sąsaja

Atliekant tyrimą vietinėje PBX sukuriami trys vartotojai, kurie bus naudojami SIP signalizavimo protokolo tyrimui 23 pav.



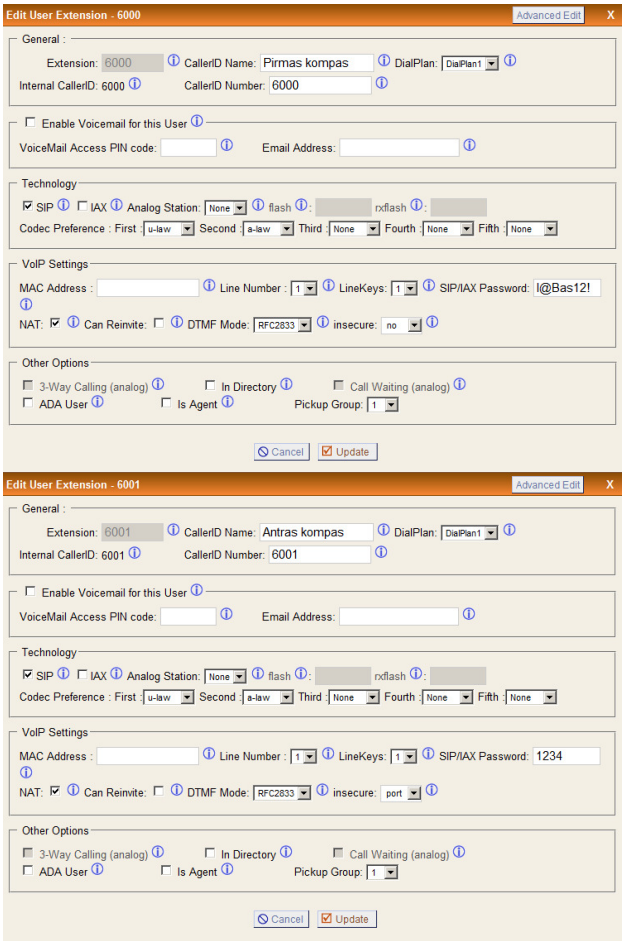
23 pav. SIP vatotojų sąrašas

Sukuriant naują vartotoją įvedama keletas nustatymų iš kurių mums labiausiai aktualūs yra vartotojo telefono numeris, kuris yra vartotojo vardas klientinėje programinėje įrangoje ir slaptažodis, kuris turėtų būti saugus 24 pav. Taip pat svarbus *insecure* parametras. Galimi trys šio parametro pasirinkimai:

- Port – leidžiamas klientų atitikimas pagal IP adresą, nereikalaujant prievado numerio atitikimo; (allows matching of peers by IP address without matching port number);

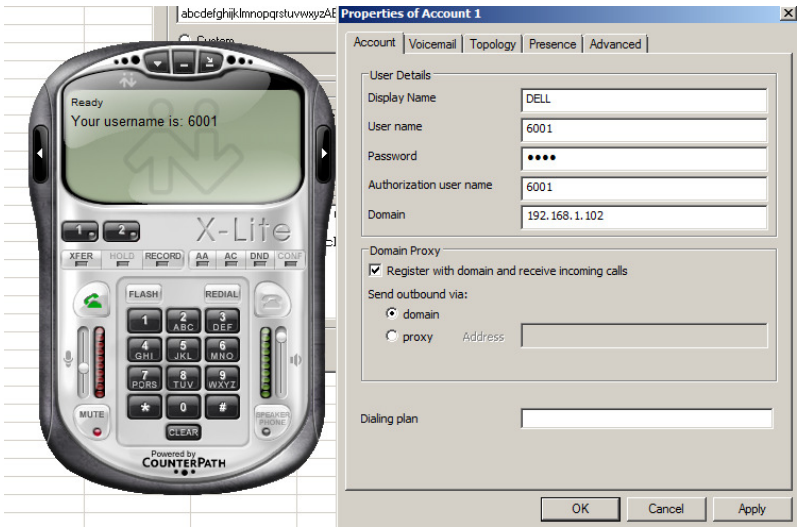
- Very - leidžiamas klientų atitikimas pagal IP adresą, nereikalaujant prievado numerio atitikimo, taip pat panaikinamas reikalavimas autentifikuoti įeinančius INVITE pranešimus;
- No – reikalauja įprasto, IP – paremto sutapimo ir autentifikuotų INVITE pranešimų; (angl. requires normal IP – based matching and autentificated INVITES).

Norint užtikrinti didžiausią apsaugą pasirenkamas *insecure* parametro reikšmė – no.



24 pav. Naujo vartotojo sukūrimas

Vartotojų kompiuteriuose įdiegiami ir sukonfigūruojami X-Lite SIP telefonai. Vartotojo vardą atitinka jo telefono numeris, o slaptažodis atitinka abonento „SIP/IAX password“ lauką naujo vartotojo kūrimo dialoge. „Domain“ lauke nurodomas Asterisk serverio IP adresas 25 pav.



25 pav. X-Lite telefono konfigūravimas

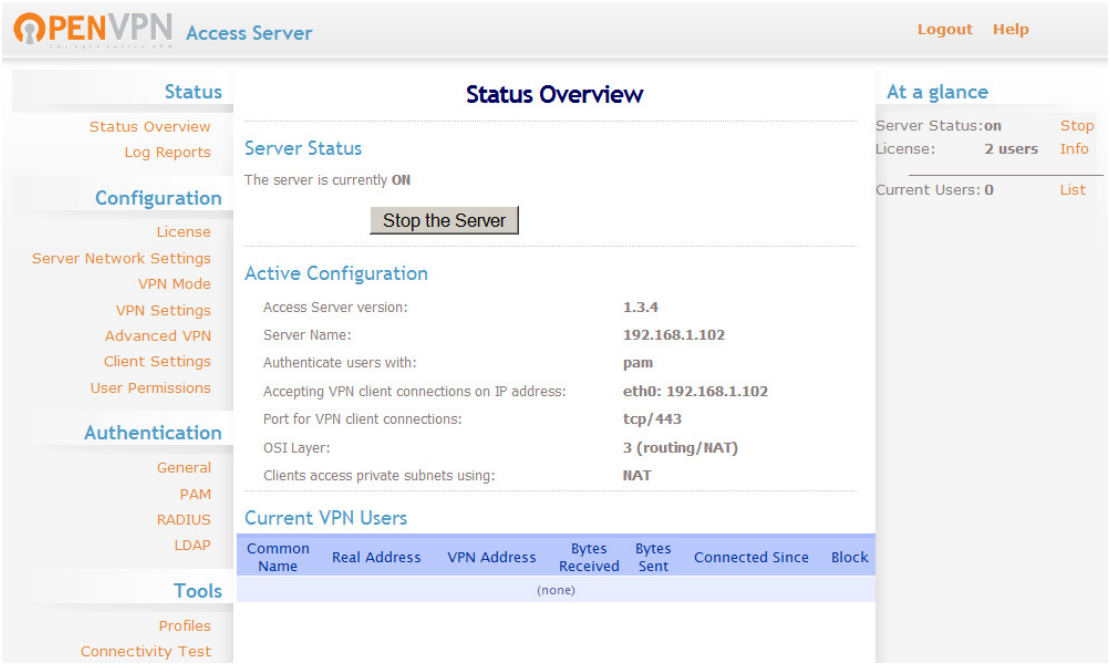
Sukonfigūravus telefoną, Asterisk serveriui siunčiamas REGISTER pranešimas, jei konfigūracija teisinga telefono būklės lange matomas pranešimas „Ready. Your username is: username“ priešingu atveju bus rodomas pranešimas „Registration error: 403 – Forbidden (bad auth)“. Jei asterisk serveris nepasiekiamas programinis telefonas rodo pranešimą Registration error: 408 – time out expired“.

4.2. OpenVPN įdiegimas ir konfigūravimas

Kadangi SIP sesijos sudarymo pranešimai tinklu perduodami atviru tekstu, todėl gali būti lengvai perimti ir modifikuoti. Norint apsaugoti tinklu perduodamus SIP signalizavimo pranešimus naudojamas saugus SIPS. SIPS protokolas aprašo SIP pranešimų perdavimą naudojant SSL/TLS (angl. Secure Session Layer/Transport Layer Security) protokolą. Tokiame tinkle, piktavalis perėmęs IP paketus, pernešančius SIP paketus, negali išsiaiškinti juose perduodamos informacijos, nes SIP yra užšifruoti. Autintifikavimui SSL/TLS naudoja X.509 protokolą, šifravimui RSA protokolą, tačiau gali būti naudojami ir kiti: DES, TripleDES ar IDEA.

Parsisiunčiame ir įdiegiame OpenVPN-AS (Access server) - tai įdiegimo ir konfigūravimo įrankis, pagrįstas populiaria OpenVPN atviro kodo programine įranga, kuris supaprastina VPN prieigos sprendimą 26 pav. OpenVPN-AS apima:

- Paprasta WEB paremta administratoriaus sąsaja konfigūravimui ir valdymui;
- lengvai naudojama grafinė OpenVPN vartotojo sąsaja;
- kliento žiniatinklio serveris, kuris automatiškai generuoja kliento konfigūraciją ir sukonfigūruotą Windows VPN kliento programinės įrangos įdiegimo bylą, po sėkmingo vartotojo prisijungimo prie serverio;
- integracija su esamomis autentifikavimo sistemomis LDAP, RADIUS, PAM.

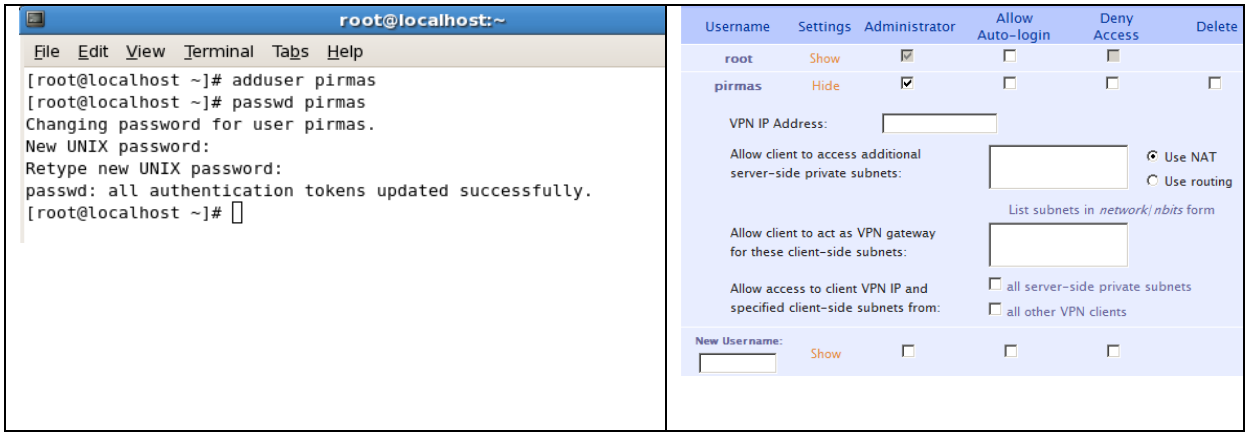


26 pav. OpenVPN-AS būsenos langas

Sukonfigūruojame OpenVPN-AS prieigos serverį:

- Pasirenkame kuriame OSI lygmenyje konfigūruojamas VPN (2 arba 3 lygmuo);
- atliekame VPN serverio tinklo nustatymus;
- nustatome vartotojų leidimus;

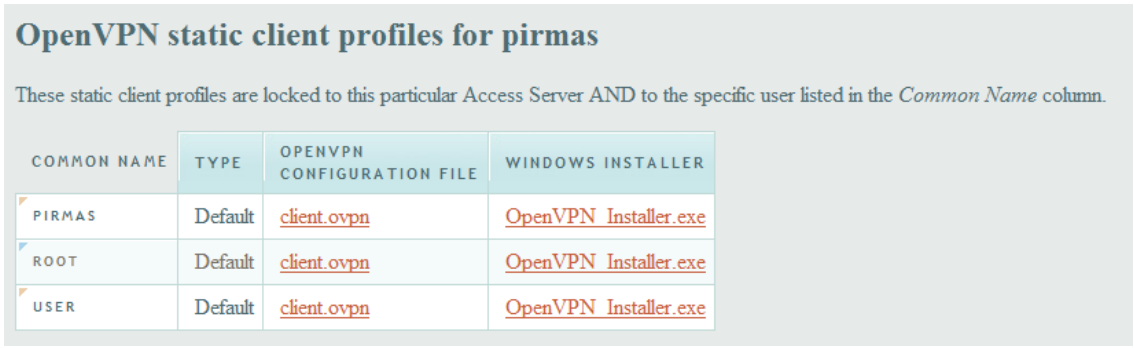
OpenVPN-AS gali dirbti dvejuose OSI modelio lygmenyse 2 – ethernet bridging arba 3 - routing/NAT. VPN tinkle naudojami 192.168.0.0 – 192.168.0.255 IP adresai. Vartotojų autentiškumo patvirtinimui naudojama PAM autentifikavimo sistema – vartotojų duomenų bazė UNIX sistemoje. OpenVPN vartotojai sukuriami panaudojant Linux komandą *adduser „vartotojo vardas“*, vartotojui sukuriamas slaptažodis panaudojus komanda *passwd „vartotojo vardas“*. Sukuriamas slaptažodis turėtų būti saugus 27 pav. Naujam vartotojui nustatome leidimus OpenVPN-AS serveryje 27 pav.



27 pav. Naujo vartotojo sukūrimas

Naudojant interneto naršyklę iš vartotojo kompiuterio jungiamės prie OpenVPN-as kliento WEB serverio. Šis serveris reikalingas vartotojų konfigūracijos failų ir kliento

programinės įrangos pateikimui vartotojams. Prisijungę sukurto vartotojo vardu ir slaptažodžiu galime parsisiųsti OpenVPN kliento programinę įrangą bei konfigūravimo bylą 28 pav.



OpenVPN static client profiles for pirmas

These static client profiles are locked to this particular Access Server AND to the specific user listed in the *Common Name* column.

COMMON NAME	TYPE	OPENVPN CONFIGURATION FILE	WINDOWS INSTALLER
PIRMAS	Default	client.ovpn	OpenVPN_Installer.exe
ROOT	Default	client.ovpn	OpenVPN_Installer.exe
USER	Default	client.ovpn	OpenVPN_Installer.exe

28 Pav. Vartotojo konfigūracijos parsiuntimas iš žiniatinklio serverio

Vartotojo konfigūracijos failas sudarytas iš Sertifikavimo centro sertifikato, vartotojo sertifikato ir privataus rakto.

Vartotojai: pirmas – KDD112@!; antras – BGF535@!

4.3. SIP signalinių pranešimų naudojant asterisk serverį tyrimas

Atliekant SIP signalinių pranešimų bei Asterisk serverio saugumo tyrimą atliekamos šios atakos:

- DoS;
- registracijos užgrobimas;
- BruteForce, žodyno ataka;

DoS atakų atveju Asterisk serveris užtvindomas SIP Invite bei Register pranešimais generuojamais piktavalio kompiuterio PC3. Asterisk serveris apdorodamas klaidingus SIP sesijos sudarymo pranešimus, sumažina VoIP paslaugų kokybę arba paslauga tampa iš vis neprieinama, priklausomai nuo siunčiamų fiktyvių pranešimų kiekio. Teisėtiems vartotojams PC1 ir PC2 kalbantis vienas su kitu nesankcionuotas vartotojas PC3 siunčia Bye pranešimą vartotojui PC1 arba PC2 taip sutrikdydamas paslaugą. INVITE, REGISTER ir BYE pranešimų struktūra pateikiama 29 pav.

```
Via: SIP/2.0/UDP 192.168.1.110:42484;branch=z9hG4bK-d8754z-704648008f40794c-1---d8754z-;rport
Max-Forwards: 70
Contact: <sip:6002@192.168.1.110:42484>
To: "6001"<sip:6001@192.168.1.102>
From: "DELL"<sip:6002@192.168.1.102>;tag=40239850
Call-ID: NjNjNzk5MzJiMzI1YjlmNDkxZmQwNTQ5MDhkMTUyZWQ.
CSeq: 1 INVITE
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, NOTIFY, MESSAGE, SUBSCRIBE, INFO
Content-Type: application/sdp
User-Agent: X-Lite release 1103k stamp 53621
Content-Length: 475
```

a)

```
Via: SIP/2.0/UDP 192.168.1.110:42484;branch=z9hG4bK-d8754z-8731b417ca72ed22-1---d8754z-;rport
Max-Forwards: 70
Contact: <sip:6002@192.168.1.110:42484;rinstance=cde90f323c89c677>
To: "DELL"<sip:6002@192.168.1.102>
From: "DELL"<sip:6002@192.168.1.102>;tag=f2624067
Call-ID: NWEzOTQwMDliMGFkZWFhMTRiY2QwMGFiOGU0ZDg5ZGQ.
CSeq: 1 REGISTER
Expires: 3600
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, NOTIFY, MESSAGE, SUBSCRIBE, INFO
User-Agent: X-Lite release 1103k stamp 53621
Content-Length: 0
```

b)

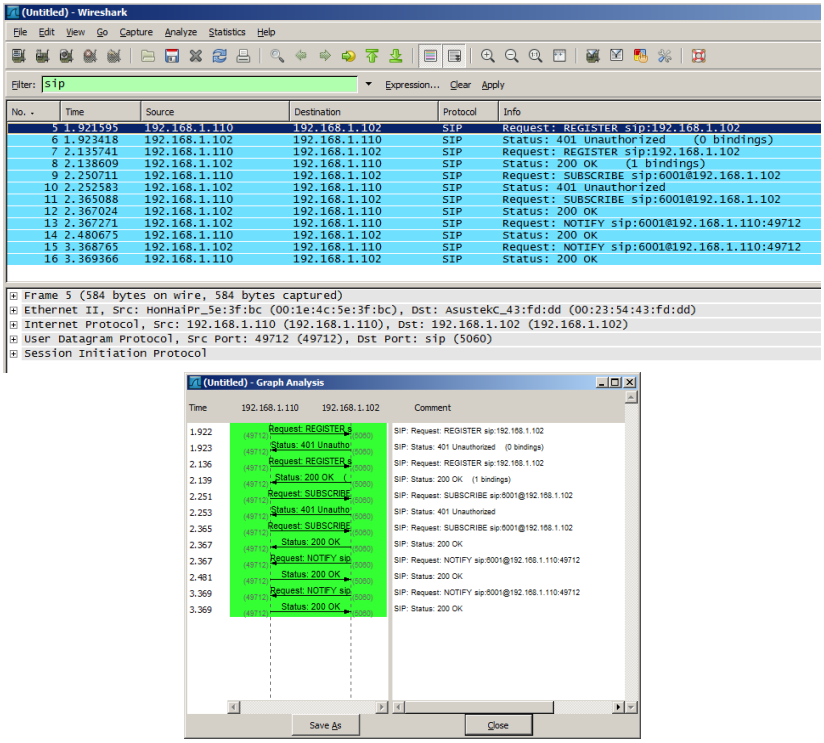
```
Via: SIP/2.0/UDP 192.168.1.110:42484;branch=z9hG4bK-d8754z-bb497673d92cb547-1---d8754z-;rport
Max-Forwards: 70
Contact: <sip:6002@192.168.1.110:42484;rinstance=cde90f323c89c677>
To: "Trecias Kompas"<sip:6002@192.168.1.102>;tag=as7785f25f
From: <sip:6002@192.168.1.110:42484;rinstance=cde90f323c89c677>;tag=d707a63f
Call-ID: 0abc1a9549be974f557e005804c24ce6@192.168.1.102
CSeq: 2 BYE
User-Agent: X-Lite release 1103k stamp 53621
Reason: SIP;description="User Hung Up"
Content-Length: 0
```

c)

29 pav. SIP pranešimų struktūra a) INVITE, b) REGISTER, c) BYE

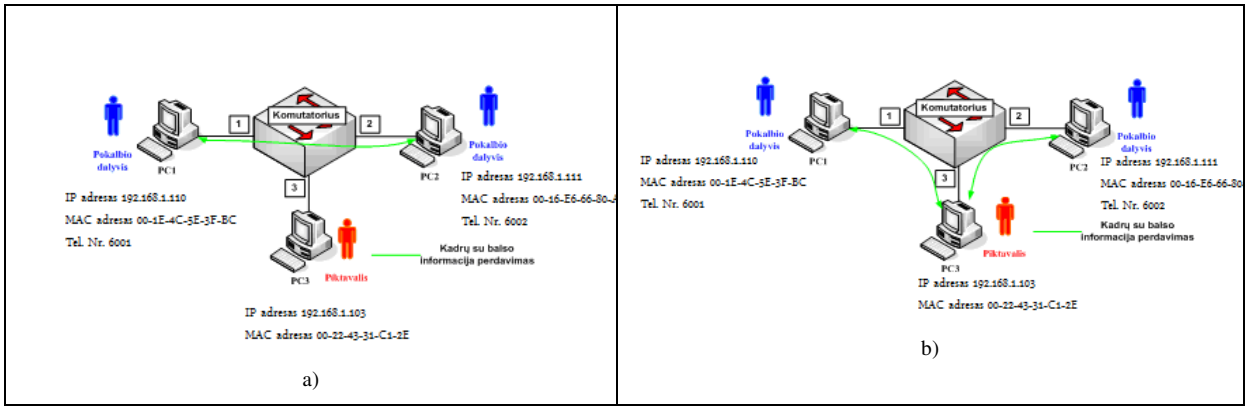
Norint prisijungti prie SIP tinko, kontroliuojamo Asterisk serverio, reikia juos priregistruoti Asterisk serveryje. Tokiu būdu vartotojas siunčia serveriui REGISTER užklausą pateikdamas vienintelį SIP varotoją identifikuojantį parametrą – vartotojo vardą. Jei registracijai reikalingas slaptažodis serveris atmeta tokią užklausą, klientui pasiųsdamas atsakymą „401 Unauthorized“. Atsakyme patalpinama informacija kaip turi būti vykdomas autentifikavimas. Nurodomas autentifikavimo algoritmas, šifravimo algoritmas, domeno vardas (realm), unikali simbolių seka (nonce), kurios galiojimas laikinas.

SIP klientas pagal gautą informaciją suformuoja naują REGISTER pranešimą. Autorizavimo informacija pateikiama laukelyje AUTHORIZATION, lauke CONTACT nurodoma kokiu adresu reikia siųsti pranešimus, kad šie pasiektų registruotą vartotoją. Asterisk serveris gavęs šį pranešimą patikrina ar autentifikavimo informacija yra teisinga, jei taip pasižymi, kad registruotas vartotojas 6001@192.168.1.102 ir jis pasiekiamas adresu 6001@192.168.1.110. Asterisk serveris siunčia SIP klientui „200 OK“ pranešimą, informuodamas, kad registracija sėkminga 30 pav.



30 pav. PC1 sėkminga registracija

SIP signalinius pranešimus gali priimti ne tik teisėtas informacijos gavėjas, bet ir piktavalis pasinaudodamas LAN, WAN tinklų pažeidžiamumais, pvz.: ARP nuodijimas 31 pav. [16] a) informacijos perdavimas tinkle, kai kompiuteriai nepaveikti ARP nuodijimu; b) informacijos perdavimas tinklu, kai kompiuteriai paveikti ARP nuodijimu.



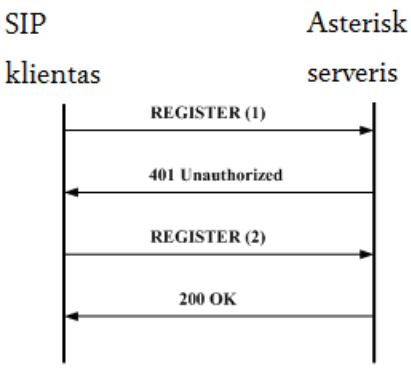
31 pav. Informacijos perdavimas a) nepaveikus ARP nuodijimu; b) paveikus ARP nuodijimu

Atliekant tyrimą Cain&Abel programoje sukuriamas ARP nuodijimo maršrutas – programoje nurodome, kad PC3 turi įsiterpti tarp Asterisk serverio ir maršrutizatoriaus 32 pav.

Status	IP address	MAC address	Packets ->	<- Packets	MAC address	IP address
Poisoning	192.168.1.102	00235443FDDD	0	0	001D0FE86A30	192.168.1.1

32 pav. „ARP nuodijimo“ maršruto sukūrimas

Perėmęs registraciją piktavalis gali užsiregistruoti kaip teisėtas vartotojas. Piktavaliui pakanka perimti antrąjį REGISTER pranešimą ir pakeisti jo CONTACT lauke nurodytą IP adresą savuoju. Asterisk serveris negali nustatyti, kad pranešimo turinys buvo pakeistas. Vartotoją identifikuojanti informacija liko nepakitusi todėl Asterisk serveris užregistruoja piktavalio SIP klientą, pasižymėdamas, kad registruotas vartotojas 6001@192.168.1.102, kuris pasiekiamas adresu 6001@192.168.1.103. Asterisk serveris piktavaliui pasiunčia „200 OK“ pranešimą informuodamas apie sėkmingą registraciją. Kad tikrasis vartotojas neįtartų, kad jo duomenimis buvo pasinaudota, piktavalis jam persiunčia „200 OK“ pranešimą CONTACT lauke nurodydamas SIP vartotojo IP adresą. Visi SIP pranešimai, kurie skirti teisėtam vartotojui, visų pirma, bus siunčiami piktavaliui, kuris gali nuspręsti ką daryti: sudaryti sujungimą, atmesti, ar perduoti SIP vartotojui. 33 pav. pateikiamas SIP kliento, o 34 pav. - piktavalio registravimosi prie Asterisk serverio procesas.



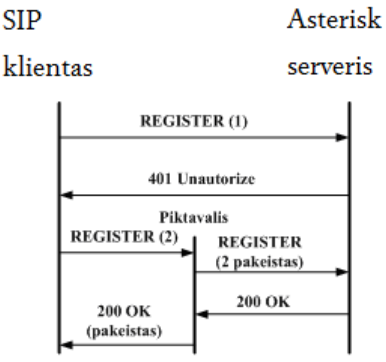

```
REGISTER sip:192.168.1.102 SIP/2.0
Via: SIP/2.0/UDP 192.168.1.110:49712;branch=z9hG4bK-d8754z-7b6fbe5a84521507-1---d8754z-;rport
Max-Forwards: 70
Contact: <sip:6001@192.168.1.110:49712;rinstance=1d40ed9e134697f0>
To: "DELL"<sip:6001@192.168.1.102>
From: "DELL"<sip:6001@192.168.1.102>;tag=c6401e55
Call-ID: NTU1MjFlOWNmYjA4NzhiNGQ2MDgxZTlhNjNjZWU4YmE.
CSeq: 1 REGISTER
Expires: 3600
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, NOTIFY, MESSAGE, SUBSCRIBE, INFO
User-Agent: X-Lite release 1103k stamp 53621
Content-Length: 0

SIP/2.0 401 Unauthorized
Via: SIP/2.0/UDP 192.168.1.110:49712;branch=z9hG4bK-d8754z-7b6fbe5a84521507-1---d8754z-;received=192.168.1.110;rport=49712
From: "DELL"<sip:6001@192.168.1.102>;tag=c6401e55
To: "DELL"<sip:6001@192.168.1.102>;tag=as003a0398
Call-ID: NTU1MjFlOWNmYjA4NzhiNGQ2MDgxZTlhNjNjZWU4YmE.
CSeq: 1 REGISTER
User-Agent: Asterisk PBX
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY, INFO
Supported: replaces, timer
WWW-Authenticate: Digest algorithm=MD5, realm="asterisk", nonce="59f69eab"
Content-Length: 0

REGISTER sip:192.168.1.102 SIP/2.0
Via: SIP/2.0/UDP 192.168.1.110:49712;branch=z9hG4bK-d8754z-3a4f5c11f6042830-1---d8754z-;rport
Max-Forwards: 70
Contact: <sip:6001@192.168.1.110:49712;rinstance=1d40ed9e134697f0>
To: "DELL"<sip:6001@192.168.1.102>
From: "DELL"<sip:6001@192.168.1.102>;tag=c6401e55
Call-ID: NTU1MjFlOWNmYjA4NzhiNGQ2MDgxZTlhNjNjZWU4YmE.
CSeq: 2 REGISTER
Expires: 3600
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, NOTIFY, MESSAGE, SUBSCRIBE, INFO
User-Agent: X-Lite release 1103k stamp 53621
Authorization: Digest username="6001",realm="asterisk",nonce="59f69eab",uri="sip:192.168.1.102",response="c9a21f6346d3d1b394e70c6c1994299e",algorithm=MD5
Content-Length: 0

SIP/2.0 200 OK
Via: SIP/2.0/UDP 192.168.1.110:49712;branch=z9hG4bK-d8754z-3a4f5c11f6042830-1---d8754z-;received=192.168.1.110;rport=49712
From: "DELL"<sip:6001@192.168.1.102>;tag=c6401e55
To: "DELL"<sip:6001@192.168.1.102>;tag=as003a0398
Call-ID: NTU1MjFlOWNmYjA4NzhiNGQ2MDgxZTlhNjNjZWU4YmE.
CSeq: 2 REGISTER
User-Agent: Asterisk PBX
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY, INFO
Supported: replaces, timer
Expires: 3600
Contact: <sip:6001@192.168.1.110:49712;rinstance=1d40ed9e134697f0>;expires=3600
Date: Tue, 26 Jan 2010 19:06:30 GMT
Content-Length: 0
```

33 pav. SIP vartotojo registravimosi procesas



```
REGISTER sip:192.168.1.102 SIP/2.0
Via: SIP/2.0/UDP 192.168.1.110:49712;branch=z9hG4bK-d8754z-3a4f5c11f6042830-1---d8754z-;rport
Max-Forwards: 70
Contact: <sip:6001@192.168.1.103:49712;rinstance=1d40ed9e134697f0>
To: "DELL"<sip:6001@192.168.1.102>
From: "DELL"<sip:6001@192.168.1.102>;tag=c6401e55
Call-ID: NTU1MjFlOWNmYjA4NzhiNGQ2MDgxZTlhNjNjZWU4YmE.
CSeq: 2 REGISTER
Expires: 3600
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, NOTIFY, MESSAGE, SUBSCRIBE, INFO
User-Agent: X-Lite release 1103k stamp 53621
Authorization: Digest username="6001",realm="asterisk",nonce="59f69eab",uri="sip:192.168.1.102",response="c9a21f6346d3d1b394e70c6c1994299e",algorithm=MD5
Content-Length: 0

SIP/2.0 200 OK
Via: SIP/2.0/UDP 192.168.1.110:49712;branch=z9hG4bK-d8754z-3a4f5c11f6042830-1---d8754z-;received=192.168.1.110;rport=49712
From: "DELL"<sip:6001@192.168.1.102>;tag=c6401e55
To: "DELL"<sip:6001@192.168.1.102>;tag=as003a0398
Call-ID: NTU1MjFlOWNmYjA4NzhiNGQ2MDgxZTlhNjNjZWU4YmE.
CSeq: 2 REGISTER
User-Agent: Asterisk PBX
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY, INFO
Supported: replaces, timer
Expires: 3600
Contact: <sip:6001@192.168.1.103:49712;rinstance=1d40ed9e134697f0>;expires=3600
Date: Tue, 26 Jan 2010 19:06:30 GMT
Content-Length: 0

SIP/2.0 200 OK
Via: SIP/2.0/UDP 192.168.1.110:49712;branch=z9hG4bK-d8754z-3a4f5c11f6042830-1---d8754z-;received=192.168.1.110;rport=49712
From: "DELL"<sip:6001@192.168.1.102>;tag=c6401e55
To: "DELL"<sip:6001@192.168.1.102>;tag=as003a0398
Call-ID: NTU1MjFlOWNmYjA4NzhiNGQ2MDgxZTlhNjNjZWU4YmE.
CSeq: 2 REGISTER
User-Agent: Asterisk PBX
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY, INFO
Supported: replaces, timer
Expires: 3600
Contact: <sip:6001@192.168.1.110:49712;rinstance=1d40ed9e134697f0>;expires=3600
Date: Tue, 26 Jan 2010 19:06:30 GMT
Content-Length: 0
```

34 pav. Piktavalio registravimosi procesas

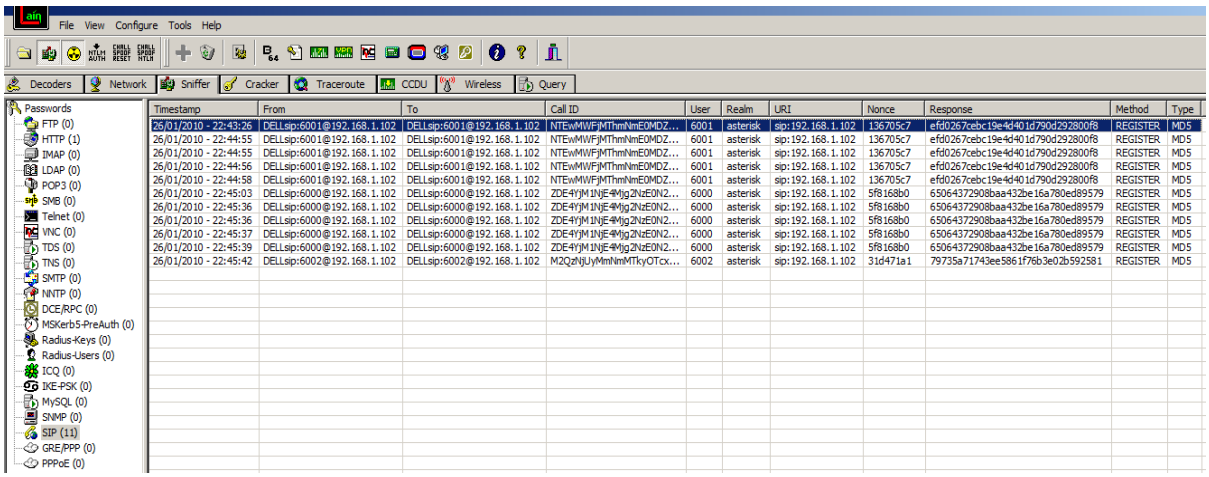
Tyrimo metu, siekiant apsisaugoti nuo registracijos užgrobimo panaudojamas OpenVPN sprendimas, perduodami SIP pranešimai yra šifruojami ir piktavalis perėmęs tokią informaciją negali išsiaiškinti ir pakeisti perduodamos informacijos 35 pav.

27	8.797798	192.168.1.110	192.168.1.102	SSL	Continuation Data
28	8.799108	192.168.1.102	192.168.1.110	TCP	https > 54063 [ACK] Seq=56 Ack=583 Win=119 Len=0
29	8.804697	192.168.1.102	192.168.1.110	SSL	Continuation Data
30	9.001435	192.168.1.110	192.168.1.102	TCP	54063 > https [ACK] Seq=583 Ack=615 Win=4212 Len=0
31	9.297642	192.168.1.110	192.168.1.102	SSL	Continuation Data
32	9.299954	192.168.1.102	192.168.1.110	SSL	Continuation Data
33	9.491436	192.168.1.110	192.168.1.102	TCP	54063 > https [ACK] Seq=1110 Ack=1174 Win=4073 Len=0
34	9.905706	192.168.1.110	192.168.1.102	SSL	Continuation Data
35	9.909973	192.168.1.102	192.168.1.110	SSL	Continuation Data
36	10.101457	192.168.1.110	192.168.1.102	TCP	54063 > https [ACK] Seq=1781 Ack=1757 Win=4380 Len=0
37	10.498648	192.168.1.110	192.168.1.102	SSL	Continuation Data
38	10.500683	192.168.1.102	192.168.1.110	SSL	Continuation Data
39	10.701439	192.168.1.110	192.168.1.102	TCP	54063 > https [ACK] Seq=2300 Ack=2316 Win=4240 Len=0
40	10.998795	192.168.1.110	192.168.1.102	SSL	Continuation Data
41	11.001214	192.168.1.102	192.168.1.110	SSL	Continuation Data
42	11.008711	192.168.1.110	192.168.1.102	SSL	Continuation Data
43	11.010753	192.168.1.102	192.168.1.110	SSL	Continuation Data
44	11.011018	192.168.1.102	192.168.1.110	SSL	Continuation Data
45	11.011087	192.168.1.110	192.168.1.102	TCP	54063 > https [ACK] Seq=3482 Ack=3913 Win=4380 Len=0
46	11.616286	192.168.1.110	192.168.1.102	SSL	Continuation Data
47	11.657243	192.168.1.102	192.168.1.110	TCP	https > 54063 [ACK] Seq=3913 Ack=3873 Win=181 Len=0
48	18.855592	192.168.1.102	192.168.1.110	SSL	Continuation Data
49	19.052028	192.168.1.110	192.168.1.102	TCP	54063 > https [ACK] Seq=3873 Ack=3968 Win=4366 Len=0
50	19.343553	192.168.1.110	192.168.1.102	SSL	Continuation Data
51	19.344669	192.168.1.102	192.168.1.110	TCP	https > 54063 [ACK] Seq=3968 Ack=3928 Win=181 Len=0

35 pav. Užšifruota SIP kliento registracija

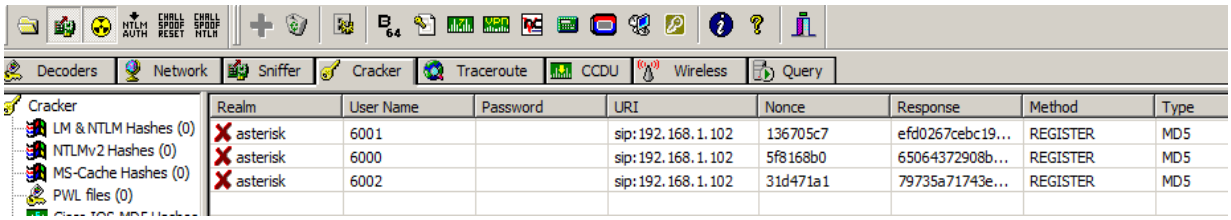
Panaudojęs ARP lentelių nuodijimą ir perėmęs SIP sesijos sudarymo pranešimus, piktavalis naudodamas žodyno ar brute force atakas gali gauti teisėto Asterisk vartotojo prisijungimo duomenis – vartotojo vardą ir slaptažodį. Gavęs šią informaciją piktavalis gali padaryti didelių finansinių nuostolių – naudodamasis šia tarnybine stotimi savo asmeninėms reikmėms arba nukreipdamas skambučių srautą per šį Asterisk serverį.

Panaudodamas Cain&Abel slaptažodžių atstatymo įrangą piktavalis „šniukštinėja“ tinklu perduodamus duomenis 36 pav.



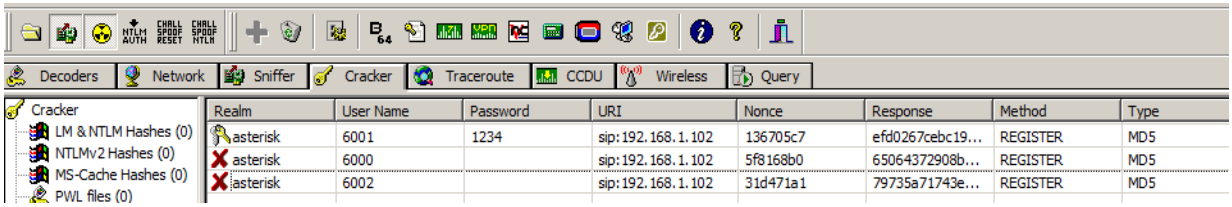
36 pav. Perimta SIP vartotojų registravimosi informacija

Susirinkęs pakankamai reikalingos informacijos piktavalis naudodamas Brute Force arba žodyno ataką bando „nulaužti“ SIP vartotojų slaptažodžius 37 pav.



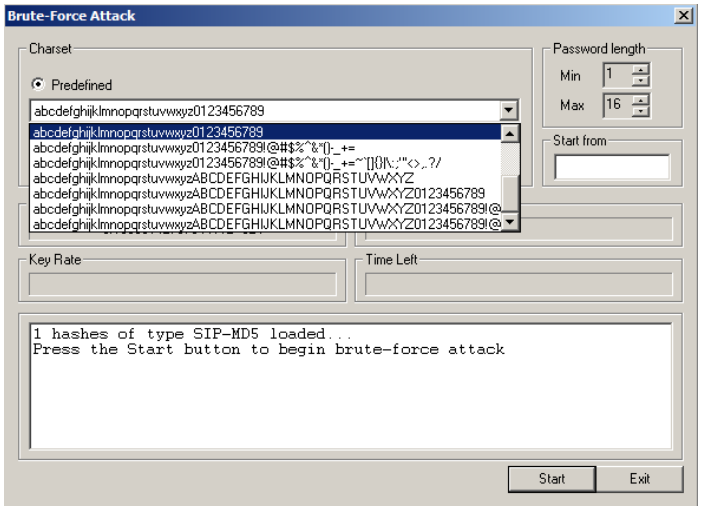
37 pav. SIP vartotojai paruošti slaptažodžio atspėjimo atakai

Parsisiunčiame žodyno atakai surengti paruoštą žodyną [7]. Šiame žodyne patalpinta 213560 skirtingų reikšmių. Ši ataka nėra sėkminga 38 pav., nes programa bando tik žodžius iš duotojo žodyno.



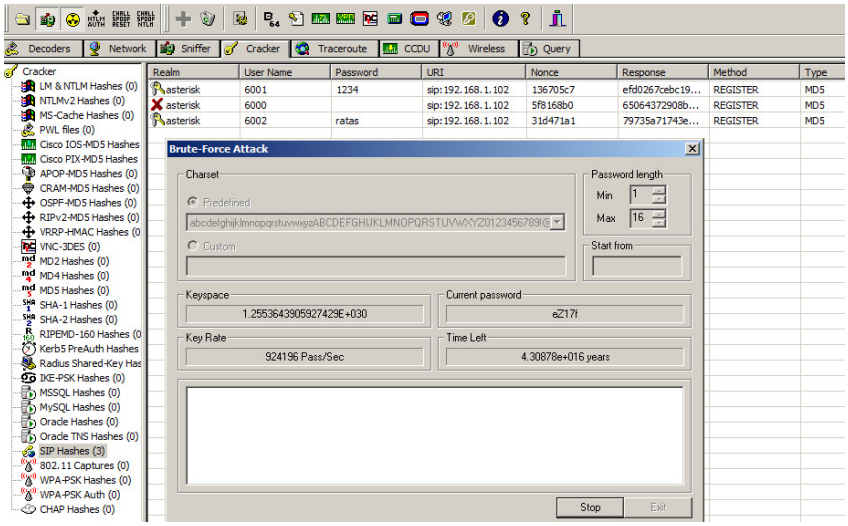
38 pav. Žodyno atakos rezultatai

Nuo šios atakos galima apsisaugoti naudojant 128 bitų slaptažodžius arba sudarant saugius slaptažodžius kurių nėra žodyne ir kurie sudaryti ne tik iš raidžių, skaičių, bet ir specialiųjų simbolių. Priešingai nei žodyno ataka Brute Force ataka perrenkamas kiekvienas galimas raktas iš duotos simbolių eilutės 39 pav.



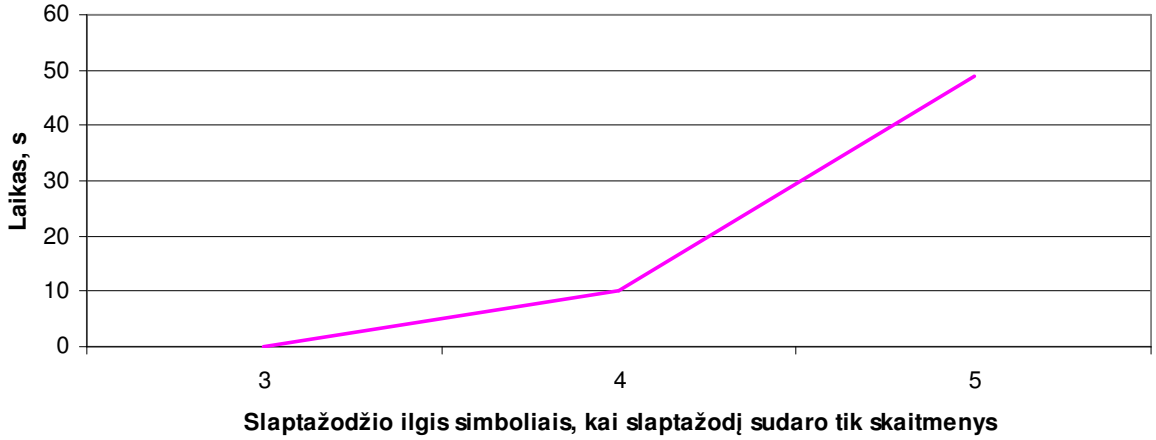
39 pav.Brute Force atakos nustatymai

Kompiuteris per vieną sekundę perrenka tūkstančius variantų ir gan greitai gali rasti reikiamą raktą. Slaptažodžio atspėjimo greitis priklauso ne tik nuo slaptažodžio sudėtingumo ir ilgio, bet ir nuo kompiuterio techninių parametrų. Šios atakos rezultatai pateikiami 40 pav.

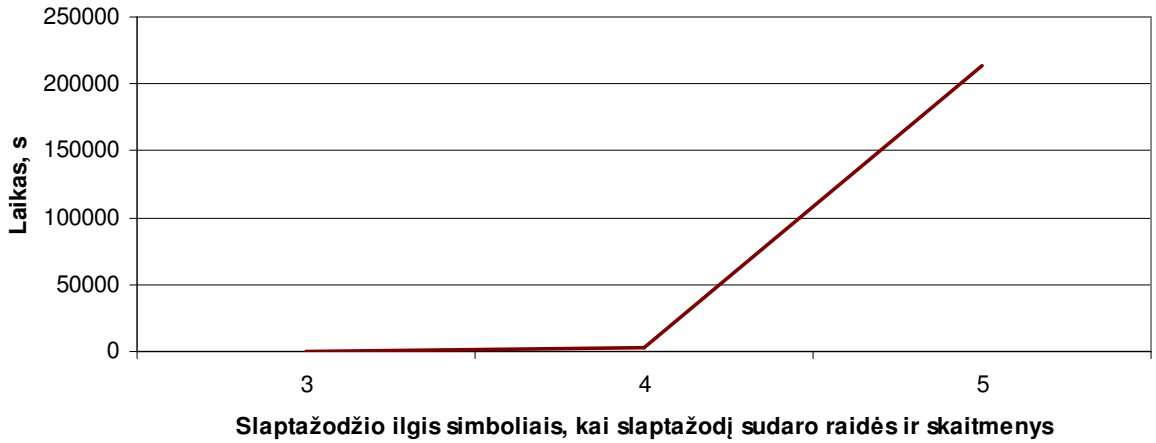


40 pav. Brute Force atakos rezultatai

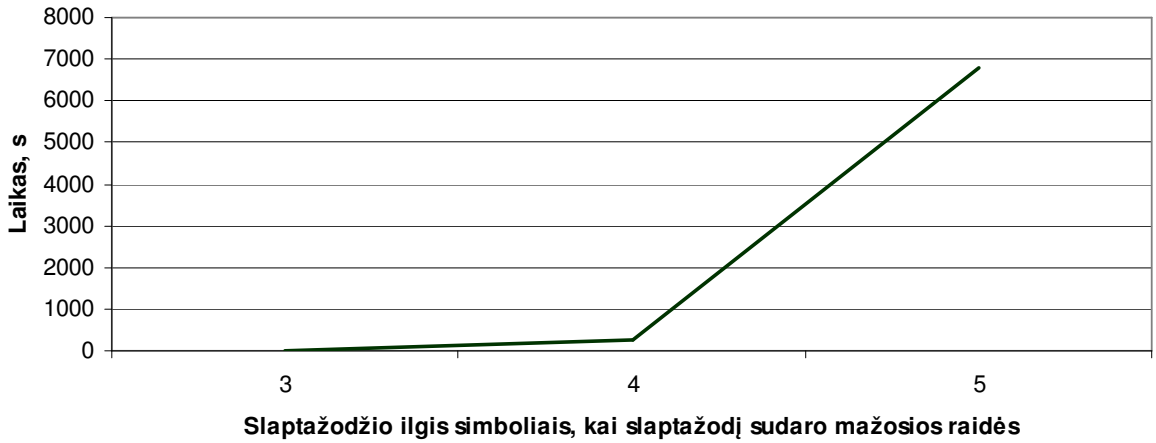
Norint apsisaugoti nuo Brute Force reikia naudoti 128 bitų ar ilgesnius raktus, tokio slaptažodžio atspėjimui pririeks labai daug laiko ir slaptažodžio panaudojimas neteks prasmės. Kaip matome 40 pav. šiuo metodu atspėti trumpi slaptažodžiai: 1234; ratas, tačiau SIP kliento kurio vartotojo vardas 6000 slaptažodžio per trumpą laiką atspėti nepavyko. Šio vartotojo slaptažodis sudarytas iš mažųjų, didžiųjų raidžių, skaitmenų ir specialiųjų simbolių – l@Bas12!. 41 pav. a, b ir c dalyse pateikiama slaptažodžio atspėjimo laiko priklausomybė nuo slaptažodį sudarančių simbolių skaičiaus, d dalyje – slaptažodį sudarančių simbolių tipo.


60
50
40
30
20
10
0
Laikas, s
3
4
5
Slaptažodžio ilgis simboliais, kai slaptažodį sudaro tik skaitmenys

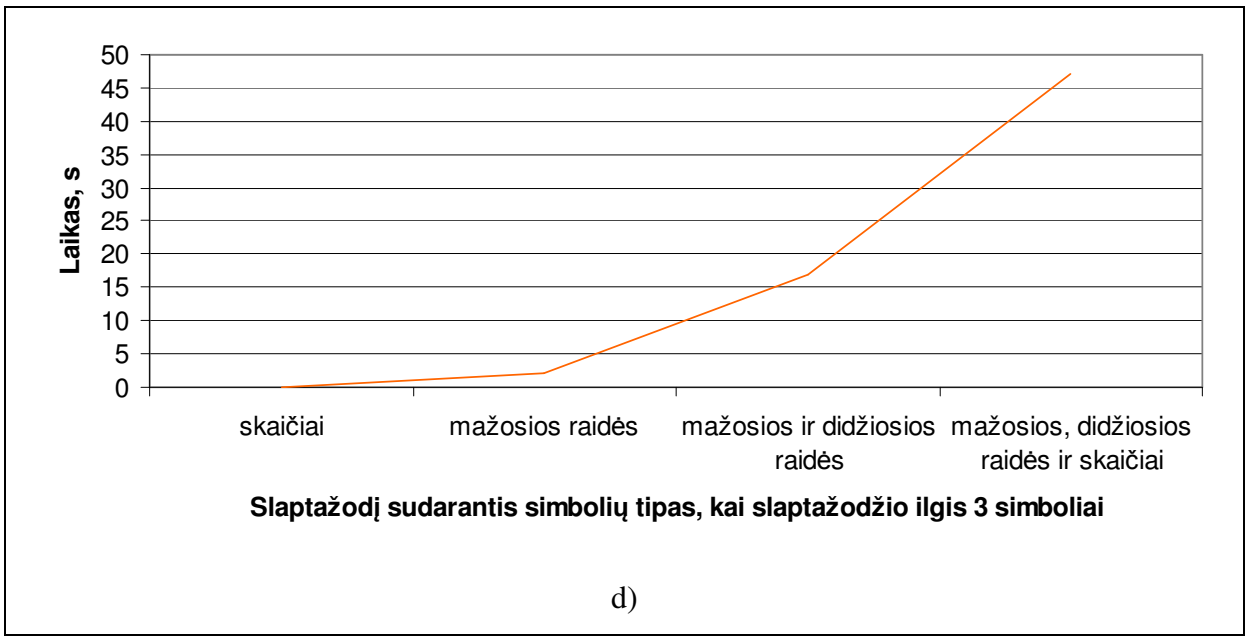
a)


250000
200000
150000
100000
50000
0
Laikas, s
3
4
5
Slaptažodžio ilgis simboliais, kai slaptažodį sudaro raidės ir skaitmenys

b)


8000
7000
6000
5000
4000
3000
2000
1000
0
Laikas, s
3
4
5
Slaptažodžio ilgis simboliais, kai slaptažodį sudaro mažosios raidės

c)

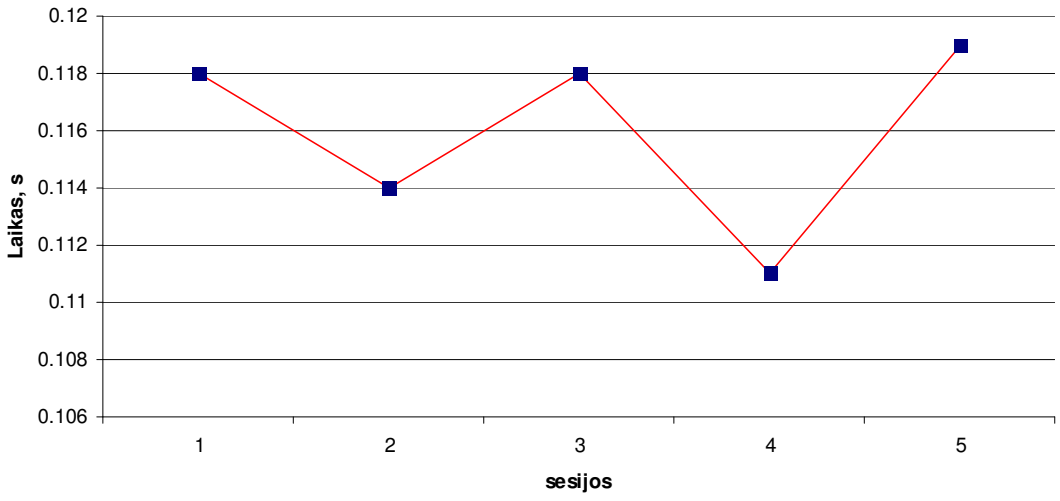


d)

41 pav. slaptažodžio atspėjimo lauko priklausomybė nuo: a, b, c - simbolių skaičiaus; d) simbolių tipo

SIP pranešimų apsaugai taip pat gali būti panaudotas OpenVPN. Naudojant saugų SIPS piktavalio programinė įranga neaptinka jokių tinklu perduodamų SIP pranešimų, todėl šie pranešimai negali būti perimti ar modifikuoti.

Išanalizavus kelias SIP sesijas Wireshark tinklo paketų analizatoriumi 42 pav. pateikiama SIP sesijos sudarymo trukmė, kai SIP signalinių pranešimų saugai nenaudojami jokie apsaugos mechanizmai.



42 pav. SIP sesijos sudarymo trukmė

Sesijos sudarymo trukmė buvo matuojama nuo INVITE pranešimo išsiuntimo iki atsakymo 180 RINGING. Įdiegus saugų SIP, sesijos sudarymo trukmės nepavyko išanalizuoti, nes tinklo duomenų paketų analizatoriumi buvo perimti šifruoti duomenų paketai, iš kurių nebuvo galima nustatyti koks signalinis pranešimas siunčiamas.

4.4. Išvados

- Ekspermentinėje modelio realizacijoje realizuotas ir ištirtas:
  - Asterisk vartotojų slaptažodžių stiprumas.
  - SIP DoS atakos.
  - SIP registracijos užgrobimas.
  - SIPS panaudojimas apsaugant SIP sesijos sudarymo pranešimus.
- Atlikus DoS atakų analizę pastebėta, kad įprastinių DoS atakų prieš Asterisk serverį galima išvengti įdiegus užkardas su atitinkamomis taisyklėmis, bei teisingai sukonfigūravus Asterisk serverį. Sudėtingiau išvengti paslaugos neteikimo atakų, kai išanalizavęs SIP pranešimų turinį piktavalis išardo legalias sesijas siųsdamas SIP BYE pranešimus.
- Analizuojat SIP tinklą pastebėta, kad SIP registracijos užgrobimas susijęs su Asterisk serverio vartotojų slaptažodžių stiprumu. Atlikęs ARP lentelių nuodijimo ataką, piktavalis perėmęs perduodamus SIP pranešimus, panaudojęs Brute force arba žodyninę ataką, gali perimti legalaus vartotojo slaptažodžius.
- Išanalizavus Open VPN panaudojimą SIP pranešimų apsaugai, t.y. SIPS, pastebėta, kad naudojantis slaptažodžių atstatymo įrankiu Cain&Abel piktavalis negali perimti ir modifikuoti tinklu perduodamų SIP sesijos sudarymo pranešimų, o tinklo paketų analizatoriumi WireShark galima stebėti šifruotus SIP pranešimus.
- Lyginant teorinio SIP tinklo modelio ir realizuoto SIP tinklo sesijos sudarymo trukmes, pastebėta, kad realaus tinklo sesijos sudarymo trukmė trunka 0,1 – 0,2 sekundes.
- Atlikus OpenVPN-AS analizę nustatyta, kad šio saugos mechanizmo panaudojimas supaprastina SIP tinklo vartotojų saugos įdiegimo procedūrą.
- SIPS panaudojimas SIP signalinių pranešimų saugos užtikrinimui reikalauja TCP protokolo panaudojimo, kuris priešingai nei UDP protokolas išnaudoja daugiau serverio resursų, todėl sesijos sudarymo laikas gali pailgėti iki 40%.
- Atsižvelgiant į eksperimentinio modelio realizacijoje naudotą kompiuterinę įrangą, išanalizuoti slaptažodžių atspėjimo laikai, kurių ilgis yra iki 5 simbolių, bei kurie sudaryti iš skaičių, mažųjų raidžių, mažųjų didžiųjų raidžių ir visų anksčiau paminėtų simbolių.
- Norint užtikrinti didesnį saugumą bei sumažinti slaptažodžių atspėjimo tikimybę, eksperimentinio modelio metu pakeisti visi naudoti numatytieji slaptažodžiai.

5. IŠVADOS

- Atlikus literatūros šaltinių analizę, paaiškėjo, kad SIP saugos užtikrinimui neužtenka vien tik Asterisk serverio teisingos konfigūracijos apsisaugant nuo SIP sesijos sudarymo grėsmių. Reikalingi papildomi saugos mechanizmai užkertantys kelią įvairioms paslaugų neteikimo, registracijos ar sesijos užgrobimo, bei kitoms atakoms susijusiomis su šiuo protokolo panaudojimu.
- Atlikus SIP protokolo analizę, pateikiami pagrindiniai: SIP tinklą sudarantys komponentai, SIP pranešimai ir atsakymai į juos, taip pat SIP sesijos sudarymo pavyzdžiai, SIP sesijos sudarymo saugumo spragos bei kovos su šiomis spragomis metodai ir priemonės.
- SIP tinklo modelis parodė, kad neapsaugoto SIP tinklo ir SIP tinklo su įdiegtais saugumo mechanizmais sesijos sudarymo laikai yra artimi 2 ms, todėl saugumo mechanizmų įdiegimas SIP sesijos sudarymo kokybei nepakenkia.
- Parenkant Asterisk serverio techninius parametrus tokius kaip atminties dydis, procesoriaus taktinis dažnis bei apkrova, turi būti atsižvelgta į šiuos parametrus: vartotojų skaičių, skambučio kokybę, skambinimo trukmę, saugumą, laiką nuo numerio surinkimo iki skambučio pradžios.
- Darbe realizuotas ir ištirtas SIP tinklas, kuriame vienu atveju SIP sesijos sudarymo pranešimai perduodami nenaudojant jokių saugos priemonių, naudojami silpni slaptažodžiai. Kitu atveju įdiegiamas SIP pranešimų saugumui užtikrinti panaudojamas SIPS protokolas, bei stiprūs SIP vartotojų slaptažodžiai. Taip pat ištirtas Asterisk serverio atsparumas DoS atakoms.
- Tyrimo rezultatai parodė, kad neapsaugoto SIP tinklo sesijos sudarymo pranešimai gali būti lengvai modifikuojami, panaudojant specialius įrankius gali būti perimta vartotojų legali registracija, taip pat sutrikdomas paslaugos teikimas, siunčiant SIP BYE pranešimus. Ištyrus SIPS panaudojimą nustatyta, kad piktavalių įrankiai neperima užšifruotų SIP pranešimų, todėl negali būti įvykdytos Brute Force ar žodyninės atakos. SIPS panaudojimas neįtakoja SIP sesijos sudarymo laiko, tačiau gali turėti įtakos tolesniam balso, vaizdo ar duomenų perdavimui.
- Tarp SIP tinklo modelio bei realizuoto SIP tinklo sesijos sudarymo laikų susidaręs skirtumas atsiranda dėl realiame tinkle esančių papildomų tinklo servisų bei apkrovų.

6. LITERATŪROS SĄRAŠAS

1. Travis Russell. Session Initiation Protocol (SIP) controlling convergent networks. McGraw – Hill Companies 2008 – 251 p.
2. Henry Sinnreich, Alan B. Johnston. Internet Communications using SIP. Wiley Publishing 2006 – 377 p.
3. Kašėta S., Adomkus T. Telefonijos informacijos ir VoIP sauga: mokomoji knyga Kaunas 2008 – 160 p.
4. Paul Mahler. VoIP Telephony with Asterisk. Signate 2004 – 247 p.
5. Thomas Porter. Practical VOIP Security. Syngress 2006 – 549 p.
6. Larry L. Peterson, Bruce S. Davie. Network Simulation Experiments Manual. Morgan Kaufmann Publishers 2003 – 161 p.
7. Mario Marchese. QoS Over Heterogeneous Networks. Wiley Publishing 2007 – 303 p.
8. William C. Hardi. VoIP Service Quality. McGraw – Hill Companies 2003 – 305p.
9. Matthew Stafford. Signaling and Switching for Packet telephony. Artech House 2004 – 245 p.
10. Jim Van Megelen, Leif Madsen, Jared Smith. Asterisk: The Future of Telephony. O'Reilly 2007 – 557 p.
11. Herculea M., Blaga T.M., Dobrota V. Evalution of Security and Countermeasures of a SIP-based VoIP Architecture. Technical university of Cluj-Napoca.
12. Ryoo J., Altoona P. S., Hwan T. Teaching IP Encryption and Decryption Using The OPNET Modeling and Simulation Tool.
13. M. Svensson. Countering VoIP Spam: Up-Cross-Down Certificate Validation. KTH information and Communication technology 2007.
14. The open source telephony project. [Žiūrėta 2009.03.10] Prieiga per internetą: www.asterisk.org
15. John Todd. Seven Steps to Better SIP Security With Asterisk. [Žiūrėta 2009.01.20] Prieiga per internetą: http://blogs.digium.com/2009/03/28/sip-security/
16. Gedmantas R. Balso informacijos aptikimo LAN tinkluose ir apsaugos nuo nesankcionuoto panaudojimo galimybių tyrimas. [Kaunas] 2007.
17. Richard Sharpe; Ed Warnicke. WireShark User's Guide. [Žiūrėta 2009.12.15] Prieiga per internetą: http://www.wireshark.org/docs/wsug_html_chunked/index.html
18. OpenVPN Access Server Guide. [Žiūrėta 2009.12.12] Prieiga per internetą: http://www.openvpn.net/index.php/access-server/howto-openvpn-as.html
19. Massimiliano Montoro. Cain&Abel User Manual. [Žiūrėta 2010.01.15] Prieiga per internetą: http://www.oxid.it/cain.html

20. Asterisk grafinės sąsajos įdiegimas. [Žiūrėta 2009.12.10] Prieiga per internetą: http://www.asteriskguru.com/tutorials/asterisk_gui.html
21. X-Lite programiniai telefonai. [Žiūrėta 2010.01.05] Prieiga per internetą: http://www.counterpath.com/x-lite.html
22. Žodyninės atakos žodynas. [Žiūrėta 2010.01.15] Prieiga per internetą: http://lastbit.com/dict.asp
23. Peter Thomas. Two attacks against VoIP. [žiūrėta 2009.01.19] Prieiga per internetą: http://www.securityfocus.com/print/infocus/1862
24. Sesijos užgrobimo ataka. [žiūrėta 2009.01.19] Prieiga per internetą: https://www.owasp.org/index.php/Session_hijacking_attack

SANTRAUKA

Magistro darbo, SIP signalinių pranešimų, naudojant Asterisk serverį, saugumo užtikrinimo tyrimas, tikslas ištirti SIP signalinių pranešimų saugumą panaudojant Asterisk serverį.

Pirmame darbo skyriuje aprašomas SIP protokolas: pagrindiniai SIP tinklą sudarantys komponentai, SIP pranešimai bei atsakymai į juos. Pateikiami įvairūs sesijos sudarymo pavyzdžiai, suderinamumas su kitomis signalizavimo sistemomis. Šiame skyriuje taip pat aptariama šio protokolo pažeidžiamumo galimybės bei saugos užtikrinimo mechanizmai.

Sekančiame skyriuje analizuojamas Asterisk serveris: kuriuose operacinėse sistemose gali būti įdiegtas, kokias paslaugas gali teikti ir kokia galinė įranga gali būti panaudota. Šiame skyriuje taip pat pateikiami 7 žingsniai norint padidinti SIP pranešimų saugumą naudojant šį serverį.

Trečioje darbo dalyje aprašomas tinklo tyrimas naudojant OPNET modeliavimo programą. Vienu atveju analizuojama neapsaugota tinklo schema, kitu atveju su įdiegtos saugos priemonėmis, bei palyginami gauti rezultatai.

Paskutiniame darbo skyriuje pateikiama atlikto eksperimentinio modelio realizacija: pasirinktų priemonių demonstravimas bei gauti rezultatai. Pateikiamos gautos darbo išvados.

ABSTRACT

The main goal of work, SIP signaling messages, using Asterisk server, security research, is to analize security of SIP signaling messages using Asterisk server.

In the first part of the work is described SIP protocol: major SIP network components, SIP messages and answers to them. Also given various sesions designs samples and compatibility with other signaling systems. SIP vulnarebility and security mechanisms are disscused in this part too.

Next chapter is used to analize Asterisk server: in which operating systems runs, what services are available and with which SIP telephones is compatible. Also seven steps to better SIP security with Asterisk server are described in this part.

The third section is used to analize network using OPNET simulation program. First of all is simulated unsecured network and after that network is simulated using security mechanisms. After simulations these results are compared with each other.

In the last part of the work is given realization of experimental model: selected security tools demonstation and received results. Also given main results and obtained conclusions.

SANTRUMPŲ IR TERMINŲ ŽODYNAS

Santrumpa	Atitikmuo lietuvių kalboje	Atitikmuo anglų kalboje
SIP	Sesijos iniciavimo protokolas	Session Initiation Protocol
RTP	Realaus laiko perdavimo protokolas	Real-Time Transport Protocol
PBX	Vietinė telefonų stotelė	Private Branch Exchange
OS	Operacinė sistema	Operating system
RFC	Techninių ir organizacinių pastabų rinkinys	Request for Comments
UAC	Vartotojo agento klientas	User Agent Client
UAS	Vartotojo agento serveris	User Agent Server
VoIP	Balso perdavimas per IP	Voice over IP
DOS	Paslaugų neteikimas	Denial of Service
IP	Interneto protokolas	Internet Protocol
IPSEC	Saugus Interneto protokolas	Internet Protocol Security
IKE	Raktų apsikeitimo protokolas	Internet Key Exchange
TLS	Transporto sluoksnio saugumo protokolas	Transport Layer Security
DNS	Srities vardų struktūra	Domain Name System
TCP	Perdavimo kontrolės protokolas	Transmission Control Protocol
UDP	Vartotojų Duomenų paketo Protokolas	User Datagram Protocol
SCTP	Srauto kontrolės perdavimo protokolas	Stream Control Transmission Protocol
PSTN	Viešasis perjungiamasis telefono tinklas	Published Switched Telephone Network
IETF	Interneto Projektavimo Specialios paskirties organizacija	Internet Engineering Task Force
VPN	Virtualus privatus tinklas	Virtual Private Network
ARP	Adreso susiejimo protokolas	Address Resolution Protocol
ICMP	Interneto kontrolės pranešimų protokolas	Internet Control Message Protocol
LDAP	Supaprastintos kreipties į katalogus protokolas	Lightweight Directory Access Protocol
RADIUS	Centralizuotos autorizacijos ir apskaitos valdymo servisas	Remote Authentication Dial In User Service
PAM	Jungimosi autentiškumo nustatymo moduliai	Pluggable Authentication Modules