И.И.Гургенидзе //Актуальные проблемы инновационного развития агропромышленного комплекса Беларуси: материалы IV-ой Междунар. науч.-практ. конф., г. Горки, 24 -26 октября 2013 г.: редкол. И.В. Шафранская (гл. ред.) [и др.].- Горки: Белорусская государственная сельскохозяйственная академия, 2013.- С. 177 -180.

5. *Королевич Н.Г.* Основные пути повышения энергетической эффективности АПК Республики Беларусь/ Н.Г. Королевич, И.А. Оганезов, И.И.Гургенидзе // Актуальные проблемы экономического развития Казахстана в условиях глобализации: материалыРеспубликанской научно-практической конференции,посвященной 50-летию образования экономического факультета, г. Астана, 17 мая 2013 г.Т. 1/ Казахский агротехнический университет им.С Сейфуллина.- Астана: КАТУ им.С Сейфуллина, 2013.- С.49-53.

6. Королевич, Н.Г. Перспективы развития нетрадиционной энергетики в сельской местности Республики Беларусь / Н.Г. Королевич, И.А. Оганезов, И.И.Гургенидзе //Актуальные проблемы формирования кадрового потенциала для инновационного развития АПК : материалы Международной научно-практической конференции (Минск, 5-7 июня 2013 г.) / редкол. : Н. Н. Романюк [и др.]. БГАТУ, 2013.- С. 184 -186.

*7. Оганезов, И.А.*Развитие ветроэнергетики в аграрных районах Гродненской области /И.А. Оганезов//Актуальные проблемы формирования кадрового потенциала для инновационного развития АПК: материалы Международной научно-практической конференции (Минск, 5-7 июня 2013 г.) / редкол. : Н. Н. Романюк [и др.]. БГАТУ, 2013.- С. 187 -190.

*8. Оганезов, И.А.*Перспективы развития ветроэнергетики на сельских территориях Республики Беларусь // Актуальные проблемы инновационного развития агропромышленного комплекса Беларуси: материалы III-ей Междунар. науч.-практ. конф., г. Горки, 16 -17 мая 2013 г.: редкой. *Шафранская И.В*. (гл. ред.) [и др.]. - Горки: Белорусская государственная сельскохозяйственная академия, 2013.- С. 194 -196.

Korolevich N., Oganezov I., Gurgenidze I.

INCREASE OF EFFICIENCY OF THE USE OF PEAT
IN AICREPUBLIC OF BELARUS

In the article the basic ways of increase of efficiency of the use of peat are examined in Republic of Belarus taking into account foreign and home advanced experience. The special attention applies on the prospects of increase of application of peat as a power medium.
The most essential events that it is expedient to carry out on home for the increase of efficiency of their work are specified in a conclusion.

ӘОЖ 681.3.053

Қазыбек Р., Байгелов Қ.Ж.

Қазақ ұлттық аграрлық университет

КОМПЬЮТЕРЛІК ЖҮЙЕЛЕРДІҢ ҚОРҒАНЫСЫН ІСКЕ АСЫРУ МОДУЛДЕРІ

Андатпа

Бұл жұмыста компьютерлік жүйелердің қорғанысын іске асыру барысында құпия идентификаторды қолдануға негізделген аутентификациялау әдістерінің бірі Kerberos хаттамасы мен шабуылды анықтау модулдері қарастырылған.

Кілт сөздер: Компьютерлік жүйе, шабуыл, қорғаныс, хаттама, идентификация, аутентификация, сервер, трафик.

Кіріспе

Қазіргі ақпараттық технологияның дамыған заманында, ақпараттық технологиялардың мүмкіндігін пайдаланушы қылмыстық топтар ойына келгенін істеуде. Нақтылап айтар болсақ, компьютерлік жүйелерден ақпараттарды ұрлау, оларды заңсыз және күшпен иемденіп алу, ақпарат қорларына қашықтан шабуыл жасауды ұйымдастыру, ақпаратты жоюды, жинау және өзгертуді мақсат ететін компьютерлік вирустарды жасап, олардың көмегімен шабуылдар ұйымдастыру. Олардың қатарында «логикалық бомбалар», «трояндық аттар», т.б. көптеген ақпараттық қарулар бар.

Компьютерлік жүйеге жасалып жатқан кез-келген шабуыл желілік трафикті немесе желілік ресурстарды талдау барысында анықталады. Сондықтан, жүйеген рұқсатсыз енуді анықтауға арналған жүйе IDS (Intrusion Detection System), анықталу деңгейлері бойынша келесі түрлерге бөлінеді: желілік және жүйелік деңгей. Желі деңгейінде шабуылды анықтау үшін өңделмеген пакеттерден тұратын деректер көзін қолдану керек. Біз құрған жүйеде шабуылды тану осы екі бағытта, желі және жүйе деңгейінде деректер мониторингін өткізетін аралас шешімдерді қолдануға негізделген.

Құпия кілтпен аутентификацияланатын хаттама

Құпия идентификаторды қолдануға негізделген аутентификациялау әдістерінің біріне Kerberos хаттамасы жатады. Kerberos хаттамасы оншақты жыл бұрын Массачусет технологиялық институтында Athena жобасының негізінде пайда болған. Бұл хаттаманы іске асыру жолдары RFC 1510 және RFC 1964 құжаттары бойынша орындалады. Мұнда Kerberos хабарламаларында қауіпсіздік мандатын жіберу форматы мен механизмдері сипатталған [1].

Kerberos хаттамасы клиент пен сервер арасында байланыс орнату алдында клиент пен сервердің өзара аутентификация жасау механизмін ұсынады. Хаттамада клиент пен сервер арасындағы ақпаратпен алмасу қорғалмаған ортада өтеді, ал жіберіліп жатқан бумалар ұсталып қалуы немесе өзгеріп кетуі мүмкін. Сондықтан бұл хаттаманы Интернет желілерінде де қолдануға болады.

Kerberos хаттамасының негізгі концепциясы екі тараптың арасында ақпаратпен алмасуды іске асыру үшін, оның екеуіне ортақ құпияны қолданып өзара куәлану мүмкіншілігіне негізделіп құрылған.

Ортақ құпиямен алмасу үшін Kerberos хаттамасы симметриялық криптография әдісін қолданады, онда шифрлеу және дешифрлеу үшін бір ғана құпия кілтті пайдаланады. Бұл кілтті білетіндігін хабар алмасушы жақ мақұлдауы тиіс.

Құпия кілтпен аутентификацияланатын хаттама, клиент серверде аутентификацияланғысы келген кезде іске кіріседі. Өзін индентификациялау үшін қолданушы аутентификаторды құпия кілтпен шифрленген деректер жиыны түрінде көрсетеді. Аутентификаторды алғаннан соң сервер оның шифрін шешіп, дешифрлеудің дұрыс орындалғанын тексеру үшін, алынған ақпаратты тексереді.

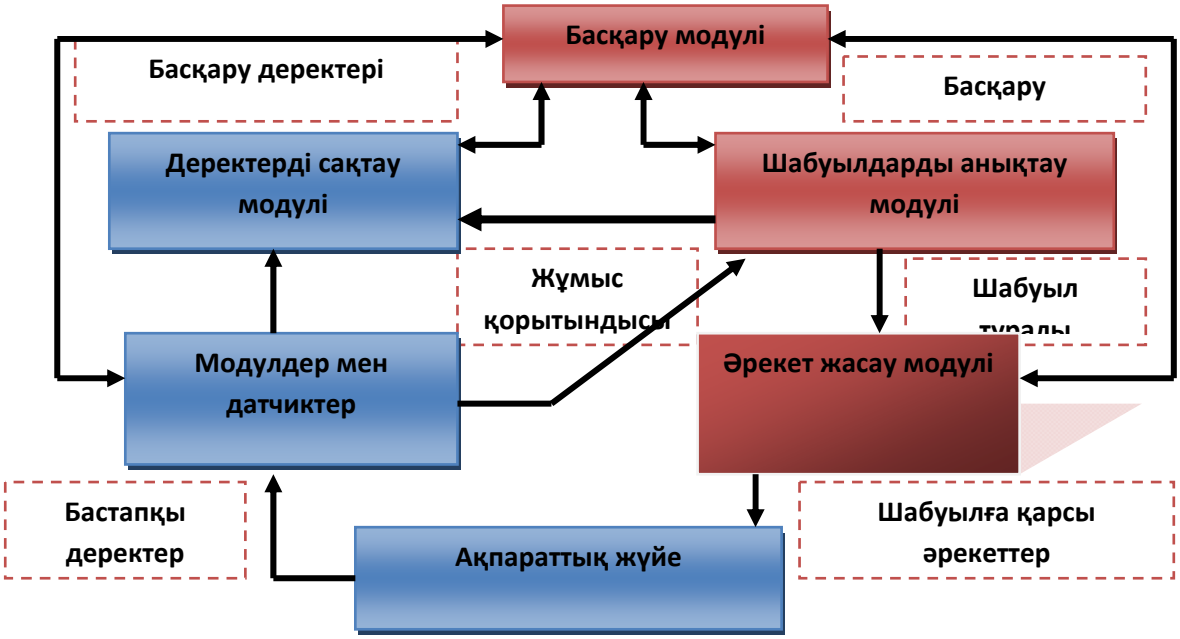
Құпия кілт желі трафигінде ұсталып қалмау үшін, кілтті келесі рет пайдаланғанда міндетті түрде өзгертіп отыру керек, сондықтан бұл шифрлеу және дешифрлеу үрдісін қайталап отыру үрдісін жеңілдету үшін, Delphi ортасында RSA стандартына негізделген программаны құрдық. Дешифрлеуден кейін тексеру дұрыс өткен болса, онда қолданушыға құпия кілт белгілі деп түсінеміз, себебі, бұл кілтті тек сервер мен қолданушы ғана білетіндіктен, тексеруден өткен қолданушының авторлығы дәлелденді деп санаймыз.

Қорғанысты күшейту үшін, сервер мен қолданушы арасында өзара аутентификация жасау керек. Бұл жағдайда сервер, бастапқы ақпараттан оның бір бөлігін бөліп алып, шифрлейді де, оны жаңа аутентификаторға айналдырып, қолданушыға жібереді. Қолданушы ақпаратты кері шифрлеу арқылы оны бастапқы ақпаратпен салыстырады, егер олар сәйкес болса, онда сервер құпия кілтті біледі деп санаймыз.

Зерттеу жүргізу барысында анықталғаны: шабуылды анықтауға арналған IDS жүйелерінің мақсаты жүйе бойында ақпаратпен алмасудың заңдылығын тексеру болғандықтан, қорғаныс жүйелерін бағдарламалық-аппараттық жиын түрінде құру керек. IDS жүйесінің жұмыс істеу алогритмі желілік экрандарға ұқсас болып келетіндіктен, бұл жүйе желілік трафикті үнемі бақылап отырады да, заңсыз қатынау орын алған жағдайда, оған қарсы шараларды іске асырады, мысалы вирустар, анықталып жойылады, ал жаңа қосылған қолданушы, міндетті түрде аутентификациядан өтуі керек [2]. Жауап беру модулі қосымша компонент болатындықтан, оны қауіп-қатерден жедел түрде құтылу үшін қолданады.

Компьютерлік желіні қорғау жүйелерін қолдану барысында Kerberos хаттамала-рынан басқа да, қорғаныс әрекеттерін жетілдіру келесі әдістермен іске асырылатыны анықталды:

- ақпараттық жүйенің құпия объекттерін ерекшелеу және топтастыру (1- сурет);



1-сурет. Шабуылды анықтау жүйесінің типтік сәулеті.

- ақпараттық жүйе элеметтерінің арасындағы және бүкіл жүйелер арасындағы ақпараттар ағынын бақылап, олардың бүтіндігін тексеріп отырудың қажеттілігі;
- периметр бойындағы жауапкершілік аймақтарын шектерге бөлу және олардың бір-бірімен ақпаратпен алмасуын, актентификациядан бастаудың қажеттілігі
- периметр бойындағы қауіпсіздік жүйелерін біртіндеп негіздеу арқылы іске асыру (мысалы, сыртқы периметр, нолдік периметр және басқалары);
- басшылардың алдында қорғанысты іске асыруды қаржылаудың қажеттілігін дәлелдеудің қажеттілігі
- барлық ерекшеленген желі периметрлері үшін қорғаныс саясатын іске асыру үшін орталықтандырылған басқарудың болуы;
- сыртқы және ішкі қорғанысты іске асыруда, бірнеше қорғаныс шектерін қолдану негізінде - компьютерлік жүйені қорғаудың эшалондалған жүйесін құру қажеттілігі;
- әр периметрді қорғау талаптарына сәйкестендірілетін, икемді және жақсы басқарылатын бақылау жүйесін енгізу;
- барлық аппараттық, бағдарламалық және апппараттық-бағдарламалық қорғаныс құралдарының барлығын қолдану, оның ішінде, деректерге физикалық қол жеткізу, желіаралық экрандарды және вирусқа қарсы күресу жүйелерін кеңінен қолдану;

- барлық қолданыстағы жетекші құжаттарда корпоративтік ақпараттық жүйелермен жұмыс барысын анықтау және онымен жұмыс істеу барысында қауіпсіздік шараларды қамтамасыз ету.

IDS жүйелерінің екі негізгі категориясы бар. Оның бірі желілік деңгейдің IDS-і, мұндай жағдайда сенсор желінің қорғалған сегментінде орналасқан хостта жұмыс істейді. Көп жағдайда сенсор ретінде бөлек алынған хосттың желілік картасы қолданылады. Ол тыңдау режимінде (promiscuous mode) жұмыс атқарады, сол арқылы желінің осы сегментінен өтетін трафикті бақылайды [3].

Хост деңгейінің IDS-і, егер сенсор хост деңгейінде жұмыс істеп жатқан болса, онда, қорғанысты іске асыру үшін келесі әдісті қолданады: операциялық жүйені хаттамалау құралдарының есептері мен қолданылып жатқан ресурстар туралы ақпаратты бақылап отыру. Желілік деңгейдегі IDS жалпы өнімділікті төмендетпейді. Бірақ хост деңгейіндегі IDS-тің шабуылды тез арада анықтайтындығына көз жеткіздік. Сондықтан, желілік деңгейде шабуылдарды анықтауға арналған арнайы программалық-аппараттық қамтамасыздандырулардың типтік архитектурасын қолдандық:

• модуль-датчиктер - желілік трафик туралы қажетті ақпаратты жинайды;

• шабуылдарды анықтау (тану) модулі-датчиктер жинаған деректерді шабуылдарды анықтау мақсатында қолданылды;

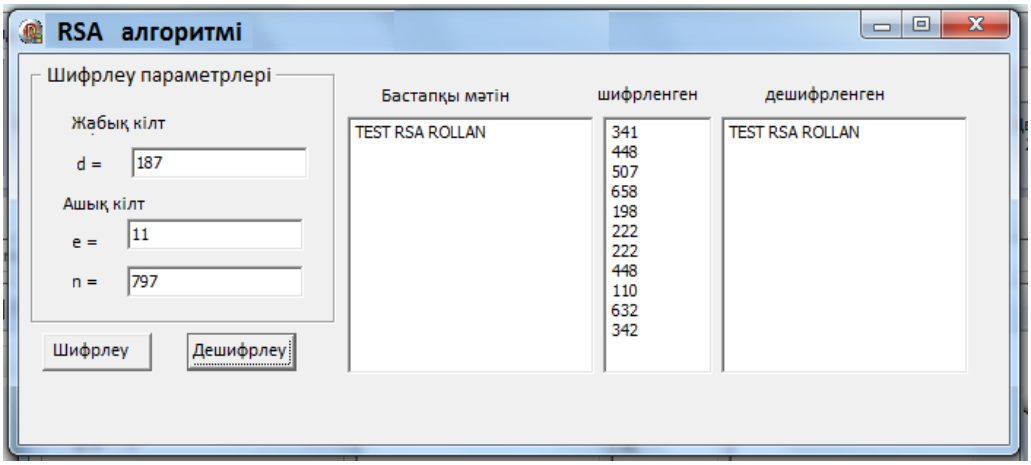
• анықталған шабуылдардың әсеріне жауап беру модулі, шабуылдарды жоюда қолданылды;

• ортаның құрылымдары туралы ақпаратты және анықталған шабуылдар туралы ақпараттарды сақтау модулі. Бұл модулде стандартты деректер қорын басқару жүйесін қолдана отырып, шабуылдар туралы ақпараттарды сақтау керек;

• IDS компоненттерін басқару модулі.

Осы аталған әрекеттерді іске асыру барысында Delphi ортасында құрылған Rollan1 программасында RSA стандарты бойынша құпия кілтті шифрлейді және жіберілген ақпаратты ашып оқу үшін, қайтадан дешифрлеуді іске асырады (2-сурет).

Сонымен, қорыта келгенде, шабуылдарды анықтау модулі IDS-тің ең қиын және ең маңызды элементі болатынына көз жеткіздік, бүкіл жүйенің тиімді жұмыс істеуі де осы модулге тікелей байланысты екені анықталды. Сондықтан, компьютерлік жүйелердің қауіпсіздігін іске асыру механизмі — ол, жүйенің ақпараттық ресурстарын пайдалану барысында максималды қорғанысты қамтамасыз етудің тиімді жолы болып табылады. Delphi-де құрылған программа, іске асырылған ұйымдастыру шаралары мен техникалық құрылғылар, бұл бірлесе атқарылатын әрекеттер, осы аталған механизмдер компьютерлік жүйе бойындағы қауіпсіздікті қамтамасыз етуші негізгі құрал болатындығы кешенді тұрғыда зерттеліп, тәжірибеде іске асырылды. Зерттеу қорытындысында, жүйе бойындағы қауіпсіздікті сақтау, оны шабуылдардан қорғау сенімді түрде іске асырылды.



2-сурет. RSA алгоритміне құрылған программаның терезесі.

Қорытынды

Компьютерлік жүйелер бойында ақпарат қауіпсіздігін қамтамасыз ету үшін, желі периметрі бойында оның барлық ерекшеліктерін есепке ала отырып, біріншіден барлық желі бойындағы ақпараттармен жұмыс істеу үшін қолданушы аутентификациядан өтуі керек, екіншіден, желі трафигіне жіберіліп жатқан шабуылдар тұрақты түрде бақыланып отыруы керек, ол үшін LanAgent жүйесін қолдандық. Сонымен, компьютерлік жүйелердің қорғанысын ұйымдастыру барысында осы қорғаныс әдістерінің барлық ерекшеліктері есепке алынып, ішкі және сыртқы периметрлерде шабуылдарды анықтауға арналған программалық-аппараттық жиыннан тұратын жүйе құрылды.

Әдебиеттер

1. *Рапх В.В.* Разработка математической модели информационного обмена в ЛВС и метода сетевой защиты информации. –М.: 2009, - 197 с.
2. *Тұрым А.Ш.* Ақпарат қорғау және қауіпсіздендіру негіздері . –Алматы:, 2002.
3. *Корнеев В.В.* Защита информации в офисе. –М.:ТК Велби, Изд-во Проспект. 2008, -333 с.

Казыбек Р., Байгелов К.Ж.

МОДУЛИ ДЛЯ ОРГАНИЗАЦИИ ЗАЩИТЫ КОМПЬЮТЕРНЫХ СИСТЕМ

Аннотация В данной работе рассматривается использование протокола Kerberos и модулей направленных на организацию защиты компьютерных систем для использования секретного индентификатора основанного на методах аутентификации.

*Ключевые слова:*Компьютерная система, атака, защита, протокол, идентификация, аутентификация, сервер, трафик.

Kazybek R., Baigelov K.

MODULE FOR COMPUTER SYSTEMS SECURITY

Annotation In this paper, we consider the use of the Kerberos protocol and modules aimed at organizing the protection of computer systems for the use of the identifier secret based authentication methods.

Keywords: Computer system, attack, defence, protocol, authentication, authentification, server, traffic.

ӘОЖ 681.3.053

Қазыбек Р., Байгелов Қ.Ж.

Қазақ ұлттық аграрлық университет

ШАБУЫЛДАРДЫ ІСКЕ АСЫРУ ҮРДІСІН МОДЕЛДЕУ ЖӘНЕ ОНЫҢ ЫҚТИМАЛДЫЛЫҚ ПАРАМЕТРІН БАҒАЛАУ

Андатпа

Шабуылдарды іске асыру үрдісін моделдеу барысы қарастырылып, осы шабуылдың пайда болу ықтималдылығының таралған заңы ретінде Пуассон заңы таңдалған, құрылған тәуекел-модель адекваттылыққа тексерілді.

Кілт сөздер: Компьютерлік жүйе, шабуыл, қорғаныс, тәуекел-модель.