**Зертханалық жұмыс №2**

**Тақырыбы:** Парольды қорғаныс

**Жұмыс мақсаты:** Бекітілмеген рұқсаттан бағдарламамен қамтамасыз ету қорғаныштарының практикалық дағдыларын алу .

Қысқаша теориялық мәліметтер.

Қорғаныс жүйелерінің қолдану қажеттілігі ( СЗ ) проблемалардың қасында шартталған, олардың арасында ерекшеленгендер: - алгоритмдерді заңсыз қолдануы,өнім аналогтерін жазғанда, автордың өзіндік интеллектуалды ойының сақталынуы (өнеркәсіптік шпионаж); бекітілмеген рұқсатты қолдану ( ұрлық және көшіріп алу); бағдарламаларға қиянат ету мақсатымен, бекітілмеген модификация қолдану; заңсыз тарату және өтім ПО (қарақшылық).

 Бағдарламалық қамтамасыз ету қорғаныштарының бар системаларын белгілері бойынша топтастыруға болады , олардың арасында құру әдісін,қолданылатын қорғаныш механизмі және жұмыс жасау принципімен ерекшелеуге болады .

Қорғаныс жүйелерін құру әдісімен жүйелерге бөлуге болады, құрылған және компиляция жасалған модульдерге; Бағдарламамен қамтамасыз етудің негізгі кодынан компиляцияға дейінгі жүйелер, және құрастырылғандар.

Бірінші үлгі жүйелері бағдарламамен қамтамасыз етуді өндірушілер үшін ең ыңғайлы,толық дайын және тесттелінген ПО-ны қорғауға жеңіл болады ( әдетте қорғаныш құру процесі автоматтандырылған және қорғайтын файл атын нұсқап және басуды көрсетеді "Enter"), сондықтан да ең әйгілі.Дегенмен,бұл жүйелердің нақтылығы төмен,қорғанышты аралап шығу үшін,"конверттік" қорғаныштың нүктесін анықтау және басқару қорғалған бағдарламаларға басқару берілуін анықтау , ал содан соң мәжбүрлі,қорғалмаған түрде оны сақтау қажет.

Жүйенің екінші үлгісі Бағдарламамен қамтамасыз етушілер үшін,ақшалы және уақытша шығындармен бағдарламалық интерфейспен жұмысқа қызметші оқыту қажеттілігі туындайды. Бірақ, осындай жүйелер шабуылдарға көбілек берік болады, себебі қорғаныш жүйесі аралық айқын шекара және сондай -ақ осында ғана жоғалады .

 Құрастырылған қорғаныш жүйелері ең ұзақ жасайтын жүйелер болып келеді. Екінші үлгі жүйелерінің адагершілік және кемшіліліктерін сақтай отырып, олар өз алгоритмдерінің дезактивациясын және анализдерді максимальді қиындатады .

Қолданылатын қорғаныш механизмдерімен СЗ қорғаныштарын топтастыруға болады : жүйелер , қолданатын күрделі логикалық механизмдар ; жүйенің , ПО-ның қолданылатын шифрлері және құрастырылған жүйелер.

Бірінші үлгі жүйелері әртүрлі әдістерді қолданады, дизассемблирования қиыншылығына бағытталғандар, жөндеулер және СЗ алгоритмы талдауының анализі және ПҚ қорғаныстары. Мына СЗ үлгісі шабуылдарға қарсы тұра алады, өйткені қорғаныш жеткілікті болуы үшін, тексеру процедураларының логикасын талдау және тиісті бейнемен оларды модификациялау қажет.

Екінші үлгі жүйелері мықтырақ болып келеді . Осындай қорғаныштардың дезактивациясына арналған дешифрация кілтін анықтау қажет.

 Құрастырылған жүйелер шабуылдарға ең берік болып келетіндер,

ПҚ-ның қорғанышқа арналған әдістерінің қатары бар, олардың ішінде:

1. *Шатастырылған алгоритмдер*-кодтың әр түрлі бөлімдеріндегі хоатикалық асулар қолданылады, -"бос нәрселер»жалған процедуралардың енгізілуі,бойдақ циклдар,процедуралардың нақты параметрлердің санының бұрмалануы,әр түрлі облыстарға код учаскелерінің шашырауы ОЗУ және т.б.

2.*Мутация Алгоритмдері* - әрбір бағдарлама жіберілген кезде айқын схемамен немесе кездейсоқ ауыстырылуы операнды – синонимдік сәйкестік кестелері туындайды және кездейсоқ өзгертілген бағдарлама құрылымдары туындайды.

3.*Компрессия мәліметінің алгоритмі*-бағдарлама буып-түйіледі , ал орындалу өлшемі содан соң шешіледі .

4.*Шифрлеу мәліметінің алгоритмі*- бағдарлама шифрленеді , ал содан соң орындалу өлшемімен шешіледі.

5.*Қорғаныш механизмінің жұмыс істеу процесіндегі күрделі математикалық айтылулардың есептеулері*-қорғаныш логикасының элементтері формулалар немесе формулалардың топтарының қандай да болмасын есептеулердің қорытындысына тәуелді болады.

6.*Дизассемблировандық әдістеме қиыншылықтары*-пакетті тәртіпте дизассемблирования қақпайлауына бағытталған әртүрлі әдістемелер қолданылады.

7.*Қиыншылық жөндеу әдісі* әртүрлі қабылдауларды жөндеулерде қолданылады , әртүрлі әдістемелер қолданылады.

8.*Операциялық жүйелер және процессорлардың эмуляциясы*- виртуалды процессор жүйелері мен операциондық жүйе жасалады( нақты бар еместер ) және ОС жүйесіне IBM жүйе командасынан бағдарлама – аударушы, мұндай аудармалар тек қана эмулятор көмегімен орындала алады , бірақ, алгоритм зерттеуіне қиындықтар келтіреді.

9*.Аппараттық* *қамтамасыз етумен стандартты емес жұмыс әдістері*- модульдік қорғаныш жүйелері ЭЕМ-лар аспабына бағытталады , операциялық жүйе процедуралары белгісіз немесе құжатқа тіркелмеген мүмкіншілікті қолданады.

Функциональдық принцип бойынша СЗ бойынша топтауға болады шифраторлар ; ( НСД ),Рұқсат етілмеген көшіру.

Ораушылар | шифраторлар. Алғашқы мақсатпен, ең басты ораушылардың бағдарлама функционалдылығына арналған зиянсыз шифраторларды тегеріште орындалатын модуль көлемінің азаюы, бірақ кейін бірінші жоспарға қорғаныш мақсаты шықты,себебі, талдауда оның алгоритмдарының және бекітілмеген модификациясының маңыздылығы басым болды. Мақсатқа осы компрессия алгоритмдары қолданылады ; мәліметтің шифрленуі , мутация алгоритмдары , бағдарлама логика бағдармасының шатастырылуы, ОС келтіруін, жұмыс уақытының стабильді еместігі және т.б .

Оң жақтары :

1. Осы жүйе ПО қоргаудың жоғары деңгейін қаматамасыз етуі- олардың алгоритмдерінің анализі болып табылады.

2.Орама әдісі басқа үлгілердің қорғаныш жүйелерінің беріктігін едәуір жоғарылатады.

Теріс жақтары:

1. Практикалық жүзді барлық әдістер, ПО кодының орындалуын бәсеңдетеді .

2. Шифрлеу | ПО код орамасы жаңарту кезінде қиыншылықтар тудырады ( update ) және қателерді дұрыстайды. ( bugfix , servicepack ).

3. Бұл жүйелер тек кішкене көлемді өнімдерге ғана қолданылады. ( 1 мегабайт ).

4. Жүйелердің тап осы класы әлсіз, дәл осылай бағдарламалық код сияқты , соңғы уақытта , шешіледі немесе таратылым орындалғанда шешіледі.

 СЗ рұқсат етілмеген көшірмеден. " бауды " дистрибутивтік сақтаушымен ( иілгіш тегеріш , қорғаныштардың CD ...). тап осы үлгісі жинақтағыштардың контроллерлерінің жұмыс зерттеуінде құрылып, жүзеге асады олардың физикалық көрсеткіштердің , - бөлу тәртіптерінде , оқудың | жазулар және т . б . мыналар жанында физикалық деңгейде дистрибутивтік сақтаушы жасалады , қожалық етуші ( болжамалы ) ерекше қасиеттермен ( мынау әдеттегі жетеді хабар сақтаушысы көмектің - белгісінің немесе | және жазуға қосымша хабардың - пароль оған немесе таңбаның ), ал модуль бағдарламада -көңілін түсірген теңестіруге және сақтаушы аутентификациясын оның бірегей қасиеттерімен жасалады. Қолдану кезінде ораушылармен | шифраторлардың әдістерін пайдалануға болады.

Оң факторлар :

1. ПО тарату және жасырын көшіріп алу қиыншылықтары;

2.ПО пайдаланушы құқықтарының қорғалуы .

Теріс факторлар :

1. Қорғаныш жүйелерін іске асырудың үлкен көлемді жұмысы ;

2.Физикалық тапсырулардың қажетті хабарларының дистрибутивтік таратылуынан сатылулардың баяулауы;

3. Қорғаныстықтың әсерінен жүйелік талаптардың жоғарылауы ( жинақтағыш барысы );

4.Аппарат пайдаланушының және қорғаныштың келіспеушілігі ( жинақтағыш , контроллер );

5. ПО жұмыс уақытында жинақтағыш шұғылданады ;

Бекітілмеген рұқсатпен ( НСД ) ПК хабарына жоспарланбаған таныстыруды , өңдеуді, көшіріп алуды, әртүрлі вирустардың қолдануын атаймыз, қиратушы бағдарламалық өнімдер соның ішінде, сонымен қатар модификацияны немесе анықталған ережелердің бұзуына рұқсат немесе шек қою.НСД-дан ПК-дағы хабарларды қорғау үшін негізгі үш бағытты ерекшелеуге болады:

Біріншіден есептеуіш ортаға бұзушыны жіберуге рұқсат етпеуі және арнайы пайдаланушының техникалықтарды тану құралдарына негізделеді;

Екіншіден есептеуіш орта қорғанышпен байланысты және арнайы бағдарламамен қамтамасыз етуге негізделеді ;

Үшінші бағыт бекітілмеген рұқсаттың ПК-дан хабарлар арнайы құралдардың қолдануымен байланысты .

НСД-дан СЗ пайдаланушының алдын ала немесе периодтық аутентификациясын жүзеге асырады немесе оның компьютерлік жүйесінің қосымша хабар сауалдары арқылы жүзеге асыруға болады. . СЗ мына үлгісіне парольды қорғаныш жүйелерін жастқызуға болады, жүйенің " баудың " пайдаланушының компьютерімен , жүйенің " маңызды тегеріштермен " және аппараттық - бағдарламалық жүйенің электрондық кілттерімен саналады. . Бірінші оқиғада " маңызды " хабарды пайдаланушы енгізеді , екіншіде - ол пайдаланушының компьютерлік жүйесінің уникальді параметрлерінің мазмұнында, үшіншіде - ол сақтаулы тегеріште және төртінші оқиғада " маңызды " хабар электрондық кілт микросхемаларынан салыстырып оқиды . Бірінші қадам, хабар қауіпсіздігі қамтамасыз етуінде шынайылықтың негізін - пайдаланушыға тексеру мүмкіншілігі келеді . Пайдаланушы адам кепілді тексеруі мақсатымен келеді және ­ теңестіру механизмдарының аутентификациясы қаралады.

Теңестіру әрбір пайдаланушыға тағайындауда негізі салынған ( пайдаланушылардың тобына ) белгіні - идентификатормен айқын айырмалықты ­ тордың және оның салыстыруда бекітілген тізіммен қаралады. Пайдаланушы адам тексеру процесінде аутентификация аталды, ол ерекшеленіп пайдаланушымен көрсетілуші арасында болады, ­ аутентификатор белгісі , оған нақты тән болады.Әрбір пайдаланушының ең басты ерекшелігі болып, аутенфикацияның эффективтілігі анықталады.

Қорғаныш хабарларының нақтылы механизмдері, яғни, аутентификация және идентификациялары келесі құралдар мен және процедуралардың болу негізінде іске асырыла алады :

Парольдер

Биометрия құралдары

Интелектуалды карталар

Автоматтандырылған жұмысшы орынның пароль арқасында немесе компьютердің блокировкаға түсуі ( клавиатураның ), бірнеше қате тіркеу кезінде пайдаланушының тұқсатына шек қойылуы мүмкін.

Криптография әрбір пайдаланушыға арналған бірегей кілттермен .

Пайдаланушылардың осындай ерекшеліктерінің сапасына байланысты,максимальді қарапайым іске асыру үшін барлығы парольдерді қолданылады . Бірақ пайдаланушылар, өзіндері жеңіл - парольдер жасауға талаптанады немесе тез табуына арналғандарды қолданады.Басқа жағынан алғанда күрделі парольдер ашық түрде жасау қажеттілігіне әкеледі .Парольды қорғаныш тек қана парольдердің жасауымен, басқару қамтамасыз етуімен тиісті өлшемдерді қабылдануын , олардың сақталуын , басылуын мезгіл өтуінің ар жағында оларды қолданудың және дер кезінде жоюлуын бақылап отыру қажет.­ Парольдердің криптографиялық жабылуы бұл проблеманы шешуді жеңілдетеді және қаскүнемдіктің алдын алуын қиындатады.

Парольды қорғаныш процедуралары орындауда қарапайым және , өндірушілер сондықтан , өте жиі қолданады . Көпшіліктері СЗбен парольдылардың кисынды механизмдерін қолданады, пароль дұрыстығы тексеруіне | кодтың және жіберуде немесе жіберілуде емес , тексеру нәтижесіне тәуелді. Қорғайтын шифрлеушілер және пароль қолданатын немесе туындыны мөлшерді одан кілт сияқты дешифрация жасайтын жүйелер де бар , сондай жүйелердің көпшілігі бағытталған шабуылдарға шифрлеу әлсіз немесе қарапайым алгоритмдары қолданады. Көпшілік құрастырушы , парольды қорғаныштар қолданатындар мына қорғаныштар- шартты - тегін бағдарламалық өнімдерге арналған қолданудың және олардың криптоалгоритмовпен берік сыпайылық орындау қиындығынан болады, компиляция жасалған модульдер тек СЗ-бен парольды соңғы кезде өңделген, оларды қорғау модульді және қосалқы кітапханалар түрінде іске асырылады және орналастырылады .

Парольды қорғаныстардың әлсізі болып енгізілген парольдың /кодтың дұрыстық тексеруі келеді. Қосымша тексерулер кезінде немесе салыстырған кезде енгізілген парольмен салыстыруға болады, жазылған кодта дұрыс немесе сгенерированным дұрыс парольмен салыстуғ болады. Мүмкін дәл осылай туынды мөлшерлердің салыстыруында енгізілген және дұрыс парольдердің , мысалы ХЭШ - функциялардың , туынды мөлшері болса кодта сақтауға болады,сонда қорғаныш беріктігі жоғарылайды. Анализ бойынша тексеру процедураларының талдауынан нақты пароль табуға болады , жазылған кодта , пароль дұрыс енгізілген немесе ХЭШ - сомамен пароль анықтамасына арналған парольдердің асып кетуіне арналған бағдарламаны жасау . Сонымен қатар , логикалық тексеруді мәжбүрлеп өзгерту арқылы СЗ шифрлеулерді қолданбай, бөгетсіз ПО рұқсатқа қол жеткізуге болады.

Авторизорлы пайдаланушымен енгізілген барлық парольды жүйелердің артынан пароль ұстап қалу қорқынышы болады. Сонымен қатар , көпшілікте тап осы үлгі СЗ ПО тексеру процедурасы қолданылады тек бір кезде , әдеттегі тіркеу жанында немесе құруға , содан соң қорғаныш жүйесі қарапайым сөнеді , немесе- заңсыз көшіріп алуда НСДқа нақты қауіп төнеді.

Оң жақтар:

1. Кәсіби емес қаскүнемнен сенімді қорғаныш.

2. Пайдаланушы үшін минимальді жағдай .

 3. Байланыс бойынша парольмен | кодты жіберу мүмкіншілігі.

4. Аппараттық қамтамасыз етумен және жүйелік және қолданбалы ПО конфликттің болмауы.

 5. Реализациямен қолданудың қарапайымдылығы.

6. Төменгі баға.

Теріс жақтары :

1. Берілген қорғаныш жүйелерінің типінің көпшілігінің төменгі бағалығы.

2. Пайдаланушы міндетті түрде пароль | кодты жадында ұстауы қажет.

Жүйенің " баудың " . Мынадай үлгі жүйелерін құру компьютерлік жүйе лердің бірегей белгілерінің іздеуін жүзеге асырады немесе олар өздері орналастырады. Кейін қорғаныш модуліін өздігінен іздеуге үйренеді және қайсыларға авторластырылған немесе авторластырымаған қолдану бұдан былай осы белгілердің теңестірілуімен анықталады. Процессор шапшаң және басқа көрсеткіштерінің бағалау әдістемелерінің қолдануы , аналық төлеулері , қосымша құрылғылардың,жадында мүмкін | микросхемалар - жадта жазу , жасырылу файлдарың жазу , ОЗУ қолдануы, ең жиі қарсы алынатын картасын күйге келтіру және т . б .қолдануға болады.

Оң факторлар :

1. Қорғаныс жұмысына арналған қосымша аппараттық құралдардың қажеті жоқ.

2. Көшірілген ПО ға бекітілмеген рұқсатың қиыншылығы.

3. Қолдану қарапайымдылығы .

4.ПО пайдаланушыға арналған «көрінбейтін» СЗ.

Теріс факторлар:

1. ПК параметрлерінде кез келген өзгертулерде СЗПО жалған жұмыстар

2. ПК пайдаланушының қаскүнем рұқсатындағы төменгі бағалылығы.

 3. ПО Жүйесімен конфликт мүмкіншілігі .

**Қорғаныc бағдарламалық - аппараттық құралдары ПО электрондық** **кілттермен.** бағдарламалық қамтамасыз ету өндірушілері арасында (ПО). Мына СЗ сыныбы үлкен әйгілілікке соңғы кезде ие болды. Арнайы құруға арналған бірді ПК стандартты порттарынан (COMM,LRT,PCMCIA,USB) немесе аналық төлеу кеңейту слоты қорғаныш бағдарламалық - аппараттық құралдары астында , бұл жағдайда, құралдың , негізі салынғандар қолдануда дәл осылай аталатындардың " аппараттықтардың ( электрондықтардың ) кілттердің ". электрондық кілт - мынау қорғаныш жүйе аппараттық бөлімі, жад микросхемаларымен төлеуді өзімен таныстырушы және оқиғалард , микропроцессормен , орналастырылғанды денеге және сондай құрылғы СМАРТ - карталарды қолданыла алады .ПО дан НСД ге өткізілген талдау нәтижелері,біреуімен қорғаныш бағдарламалық - аппараттық құралдардың қорғаныштың ең берік жүйелерінің бірі болып табылады.

Электрондық кілттерді сәулетіне байланысты жадпен кілттерге бөлуге болады ( микропроцессорсыз ) және кілттер микропроцессормен (және жадпен ).

Бірінші үлгі типі аппараттықпен жүйелердің ең бастысы. Сондай жүйелерде сын хабар ( дешифрации кілт , асулардың кестесі ) электрондық кілт жадында сақталады. Сондай қорғаныштардың дезактивациясына арналған қаскүнемнің аппраттық бөлімі бар жағдайда қажетті қорғаныш жүйелері бар. ( негізгі әдістеме : диалог ұстап қалуы аралық бөлімдермен бағдарламалық және аппараттықпен сын хабардың рұқсатына арналған ).

Ең беріктер ақпараттық жүйе екінші үлгі типімен сәйкес келеді . Дешифрации кілті тек қана кешенді аппараттық бөлімде асырайды , сонымен қатар шифрация одақтары | тап осы дешифрациилардың , сайып келгенде электрондық кілтке қорғаныш жұмысы жанында шифрланған хабар одақтарға беріледі , ал шифрі ашылғаннан қабылданады . Дәл осылай мына үлгі жүйелерінде дешифрации кілті жеткілікті күрделі жолдан ұстап алу қалай барлық процедураның іске асырылуы аппараттық бөліммен, бірақ қорғаныш жүйелері еңбекпен өтеуден кейін ашық түрде қорғалған бағдарлама мәжбүрлікпен сақтау мүмкіншілігімен қалады. Сонымен қатар, оларға криптоанализ әдістері қолдануға болады.

Оң факторлар:

1. ПҚ қолданудың және заңсыз таратудың маңызды қиыншылықтары;

2. ПҚ өндірушіден құтылу өңдеуден өзіне меншікті жүйелердің қорғанышы;

3. ПҚ қорғаныс биік автоматизацияланған процесі;

4. Демо - болжамаларды жеңіл жасау мүмкіншілігі;

Теріс факторлар :

1. СЗ нің шектелгендігінен жоспардың қиындауы;

2. Қызметшілерді оқытуға; қорғаныш жүйесін сатып алуға қосымша шығынның шығуы;

3. Қорғаныштықтан жүйелік талаптардың жоғарылауы (сыйысушылық , драйверлер );

4. ПҚ-ның қолданбалы пайдаланушыдан немесе қорғаныш жүйелерінің келіспеушілігі;

5. Пайдаланушының аспабының және аппаратурасының келіспеушілігі;

6. Аппараттық кілттің ұрлану кауіптілігі

**1. ПҚ ның қорғаныс құралы " маңызды тегеріштермен ".** Қазіргі уақытта мына қорғаныш жүйелерінің типі үлгісі аз таралған,оның моральді ескіруіне байланысты . Көптеген электрондық кілттермен жүйелерге ұқсас , бірақ сын хабар осында арнайы , маңызды таратушыда сақталады.

**Тапсырма.** Индивидуалды вариантпен сәйкестендіре бағдарламаларды жазу

|  |  |
| --- | --- |
| Нұсқа | Тақырыптары |
| 1 | «Шатастырылған» алгоритмді қолдану арқылы бағдарламаны қорғау |
| 2 | «Мутациялық» алгоритмді қолдану арқылы бағдарламаны қорғау |
| 3 | Бекітілмеген рұқсаттың қолдану арқылы бағдарламаны қорғау.Парольді қорғау |
| 4 | Бекітілмеген рұқсатты қолдану арқылы бағдарламаны қорғау.Парольді код ПО |
| 5 | Бекітілмеген рұқсатты қолдану арқылы бағдарламаны қорғау.Парольді қорғау. Пароль ХЭШ суммасына негізделген. |
| 6 | Бекітілмеген рұқсатты қолдану арқылы бағдарламаны қорғау.Парольді қорғау. Шифрленген пароль. |
| 7 | Бекітілмеген рұқсатты қолдану арқылы бағдарламаны қорғау.Парольді қорғау. ПО және ПК жолымен |
| 8 | Бағдарламадағы ерекшелік белгілері. |

**Бақылау сұрақтары:**

1. ПҚ ның бағдарламалық қамтамасыз ету қорғаныштарының классификациялық принциптері

2. Қорғаныш жүйелерінің таптастыруы ПҚ ның құру әдісімен қорғаныш жүйелерінің классификациясы

3.ПҚ-ның қорғаныштағы қолданылатын механизмдерінің классификациясы

4. ПҚ ның функциональді принципі бойынша қорғаныш жүйелерінің классификациясы

5.Ораушы- шифраторлардың тағайындалуы

6. Бекітілмеген рұқсаттан көшіріп алудың қорғаныш жүйесі

7. Бекітілмеген рұқсаттан қорғаныш жүйесі

8. Компьютермен ПҚ ның жүйелілік байланыстың жүйесі

9. Электрондық кілттермен қорғаныш жүйесі.