ӘОЖ 651.928

ДЕРЕКТЕР БАЗАСЫНДАҒЫ КРИПТОГРАФИЯ

Мэлсова Н.Ш., 2 курс, 7М06101 – бизнес, информатика мамандығы, Х.Досмұхамедов атындағы Атырау университеті, Атырау қаласы
Махатова В.Е., тех.ғ.к., профессор, Х.Досмұхамедов атындағы Атырау университеті, Атырау қаласы

Бұл мақалада пайдаланушыларды аутентификациялау, рұқсатсыз қараудан қорғау үшін пайдаланушы деректерін шифрлауға деректер базасының серверлерінде криптографиялық әдістерді пайдалану талқыланады. Кестелерге жолдар салынған кезде деректерді шифрлау үшін MS SQL Server дерекқор серверінде арнайы шифрлау функцияларын қолдану қарастырылады.

Қазіргі уақытта адамзат объектілер мен құбылыстар туралы ақпараттың үлкен көлемін жинақтады, олар электронды түрде сақталады және дерекқорларда пайдаланылады, оларды қорғау жергілікті, корпоративтік және жаһандық желілерде көп пайдаланушыға қол жеткізу мүмкіндігіне байланысты ақпараттық қауіпсіздік мәселелерін шешудегі басты проблема болып табылады.

Ақпараттық ресурстарды тиімді қорғауды қамтамасыз ету іс жүзінде кез келген қызмет салаларында аса маңызды ақпараттың құпиялылығын сақтаудың қажетті шарты ретінде кешенділіктің жоғары критерийлерін сақтауды көздейді. Деректер базасының қауіпсіздік жүйесі ақпаратты қорғаудың кешенді шешімі болып табылады. Криптография осындай кешенді қорғаудың бір бөлігі ғана. Көп деңгейлі қауіпсіздік жүйесінде бұл ішкі қорғаудың соңғы деңгейі. Ол пайдаланушыларды аутентификациялау, жасалған әрекеттен бас тарту мүмкін еместігі (non-repudiation), рұқсатсыз қараудан қорғау үшін пайдаланушы деректерін шифрлау үшін қолданылады.

Криптографиядағы шифрлау-бұл кілт немесе пароль арқылы деректерді жасыру әдісі, яғни аса маңызды деректерді шифрланған түрде сақтау және беру. Бастапқы деректерді шифрлау үшін тиісті кілтті немесе парольді білмей шифрланған мәліметтерден алу мүмкін емес. Симметриялық (бір түйінді) және асимметриялық (екі түйінді) криптожүйелерді де қолдануға болады. ДБ серверлерінде ДБ-ға қосылу кезеңінде пайдаланушыларды сәйкестендіру және аутентификациялау (түпнұсқалығын тексеру) жүргізіледі. Болашақта пайдаланушы немесе процесс өзінің мәліметтер жиынтығына сәйкес деректерге қол жеткізе алады. Пайдаланушының дерекқорға қосылуы үзілген жағдайда, ағымдағы транзакция кері қайтарылады және қосылымды қалпына келтіру кезінде пайдаланушыны қайта сәйкестендіру және оның өкілеттіктерін тексеру қажет. Сәйкестендіру мен аутентификацияның ең көп таралған тәсілі-атау мен парольді пайдалану. Бұл ақпарат субъект рұқсат етілген пайдаланушы болып табылатындығын анықтау үшін жүйемен бағаланады. Деректер базасының серверлерінде парольдер шифрланған түрде сақталады.

Қазіргі әлемде құжаттардың электрондық нысандары (соның ішінде құпия) мен оларды өңдеу құралдарының кеңінен таралуымен қағазсыз құжаттаманың түпнұсқалығын және авторлығын белгілеу проблемасы ерекше өзекті болды. Бас тарту мүмкін еместігі туралы талапты орындау кез-келген адамға белгілі бір файлды немесе деректерді жібергенін немесе алғанын жоққа шығаруға мүмкіндік бермейді. Кәдімгі хаттың немесе құжаттың соңында орындаушы немесе жауапты адам қолын қояды. Электрондық құжаттың соңында асимметриялық криптоалгоритмдерді пайдалануға негізделген цифрлық қолтаңба алгоритмін қолдана отырып алынған электрондық цифрлық қолтаңба қойылады. Мысалы, DSS (Digital Signa-

ture Standard) стандартындағы DSA (Digital Signature Algorithm) цифрлық қолтаңба алгоритмі. Даулар туындаған кезде қол қоюдан бас тарту мүмкін емес, себебі оның орындалмауына байланысты ашық кілтті білетін кез келген абонент қолының түпнұсқалығын тексере алады.

Сертификаттар-бұл қосымша метадеректері бар асимметриялық кілттер. Бұл метадеректерге аяқталу уақыты және осы сертификатты берген сертификаттау орталығы сияқты ақпарат кіреді. Егер деректерді жіберуші немесе алушы өзі берген адам екеніне көз жеткізу қажет болса, сертификаттар бұл мәселені шешуге көмектеседі. Сертификаттау орталықтары оған тапсырыс берген пайдаланушыға жіберілетін қолтаңбасы бар сертификат жасайды. Ол деректерді жіберу үшін осы сертификатты пайдаланған кезде, алушы оны сертификаттау орталығында тексеріп, жіберушінің түпнұсқалығын тексере алады. Сертификаттар мен кілттердің айырмашылығы-олар жұмыс істейтін уақыт аралығы және сертификат иесін көрсететін ерекше метадеректер. Бар самозаверительные сертификаттар. Мысалы, MS SQL Server өзінің соңғы нұсқаларында алғаш рет іске қосылған кезде автоматты түрде өздігінен қол қою сертификатын жасайды. Бұл сертификат MS SQL Server аутентификациясын орындау кезінде қосылымды шифрлау үшін қолданылады.

TDE (Transparent Data Encryption) – деректерді ашық шифрлау. Деректерді мөлдір шифрлау (TDE) – симметриялық кілттің көмегімен шифрлаудың ерекше жағдайы. TDE дерекқорды шифрлау кілті деп аталатын симметриялы кілтті пайдаланып дерекқорды шифрлайды. Дерекқорды шифрлау кілті басқа кілттермен немесе сертификаттармен қорғалған, олар өз кезегінде Дерекқордың негізгі кілтімен немесе кеңейтілген кілттерді басқару модулінде сақталған асимметриялық кілтпен қорғалған. Деректер жедел жадтан дискіге жазылса, олар шифрланады. Деректер жедел жадқа қайта жүктелген кезде, олар шифрланады. Осылайша, дискідегі деректер шифрланған, бірақ жедел жадта жоқ. TDE-нің басты артықшылығышифрлау және шифрлау қосымшалар үшін мүлдем ашық. Енгізу-шығару операцияларындағы деректер файлдары мен транзакция журналдарын шифрлау және шифрлау нақты уақыт режимінде жүзеге асырылады. Аталған шифрлау әдістерін деректерді ұйымдастырудың әртүрлі деңгейлерінде қолдануға болады. Болады шифрлау деректер базасын тұтас, жекелеген кестелер (мәнін) немесе қолдануға шифрлау жекелеген бағандар (атрибуттар).

Симметриялық деректерді шифрлау кілтін жасыру үшін арнайы функцияларды қолдана отырып шифрлау екі деңгейлі кілт иерархиясын қолданады. Мөлдір шифрлау технологиясында кілттердің сенімділігі үшін әлдеқайда күрделі кілттер иерархиясы қолданылады. Мысалы, MS SQL Server – де ол келесідей жасалады: – TDE көмегімен шифрланған әр дерекқор үшін арнайы кілт жасалады-Database Encryption Key (DEK). Бұл кілт деректерді шифрлау үшін қолданылады; – Database шифрлау кілті (DEK) master дерекқорында алдын – ала жасалуы керек сертификатпен шифрланған; – бұл сертификат master DB негізгі кілтімен шифрланған; – master DB негізгі кілті (Data Master Key-DMK) қызметтің негізгі кілтімен шифрланған (Service Master Key немесе SMK); – қызметтің негізгі кілті (SMK) DPAPI (Data Protection API) арқылы шифрланған. Мұндай схема MS SQL Server-ге кез-келген уақытта мәліметтер базасы шифрланған кілтке, демек, шифрланған деректерге қол жеткізуге мүмкіндік береді. Мұндағы ең әлсіз байланыс-бұл кілт иерархиясының жоғарғы жағында орналасқан және DPAPI көмегімен қорғалатын қызметтің негізгі кілті (SMK). Ол қажет болған жағдайда автоматты түрде жасалады, бірақ оны өзгертуге, сақтауға және қалпына келтіруге болады. Барлық басқа кілттер мен сертификаттар жасалуы керек. Басқа дерекқор серверлерінде мөлдір шифрлау технологиясының кілт иерархиясы кейбір айырмашылықтарға ие. Қарастырылған кірістірілген криптографиялық құралдар бір-бірін өзара толықтырады және дерекқорды кешенді қорғаудың ажырамас бөлігі болып табылады, онсыз деректерді сенімді қорғауды ұйымдастыру мүмкін емес.

Аталған шифрлау әдістерін деректерді ұйымдастырудың әртүрлі деңгейлерінде қолдануға болады. Болады шифрлау деректер базасын тұтас, жекелеген кестелер (мәнін) немесе қолдануға шифрлау жекелеген бағандар (атрибуттар). ДБ серверлерінде криптографиялық қорғауды пайдалану кезінде басшылыққа алуға ыңғайлы ережелерді тұжырымдаймыз: шифрланған мәтіннің екілік кодының ең күрделі немесе ұзын тізбегін алу үшін ұзақ шифрлау кілттерін пайдалану керек; ассиметриялық шифрлауда кілттер жұбын пайдалану (бір ғана кілт пайдаланылатын симметриялық шифрлаумен салыстырғанда) зиянкес үшін криптоанализдің күрделілігін арттырады; блоктық шифрлар ағындық шифрларға қарағанда сенімдірек; асимметриялық шифрлау жүйені баяулатады, сондықтан көптеген деректерді шифрлау үшін оны пайдаланбау керек. Симметриялық шифрлау осы мақсатқа жақсы сәйкес келеді; ұзын күрделі парольдер қысқа парольдерге қарағанда сенімді.

Симметриялық деректерді шифрлау кілтін жасыру үшін арнайы функцияларды қолдана отырып шифрлау екі деңгейлі кілт иерархиясын қолданады. Мөлдір шифрлау технологиясында кілттердің сенімділігі үшін әлдеқайда күрделі кілттер иерархиясы қолданылады. Мысалы, MS SQL Server – де ол келесідей жасалады: TDE көмегімен шифрланған әр дерекқор үшін арнайы кілт жасалады-Database Encryption Key (DEK). Бұл кілт деректерді шифрлау үшін қолданылады; Database шифрлау кілті (DEK) master дерекқорында алдын – ала жасалуы керек сертификатпен шифрланған; бұл сертификат master DB негізгі кілтімен шифрланған; master DB негізгі кілті (Data Master Key-DMK) қызметтің негізгі кілтімен шифрланған (Service Master Key немесе SMK); қызметтің негізгі кілті (SMK) DPAPI (Data Protection API) арқылы шифрланған. Мұндай схема MS SQL Server-ге кез-келген уақытта мәліметтер базасы шифрланған кілтке, демек, шифрланған деректерге қол жеткізуге мүмкіндік береді. Мұндағы ең әлсіз байланыс-бұл кілт иерархиясының жоғарғы жағында орналасқан және DPAPI көмегімен қорғалатын қызметтің негізгі кілті (SMK). Ол қажет болған жағдайда автоматты түрде жасалады, бірақ оны өзгертуге, сақтауға және қалпына келтіруге болады. Барлық басқа кілттер мен сертификаттар жасалуы керек.

Пайдаланылған әдебиеттер тізімі

1. Л.К. Бабенко, Е.А. Ищукова «Современные алгоритмы блочного шифрования и методы их анализа» / М., 2006

2. А.В. Маркин «Построение запросов и программирование на SQL» / М., 2008

3. Л. Бейли «Изучаем SQL» / Питер, 2012

4. G. Singh, A. Supriya «Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security», 2013

УДК 621.391

РАЗРАБОТКА ТЕХНОЛОГИЧЕСКИХ РЕКОМЕНДАЦИЙ ПО ПОВЫШЕНИЮ НАДЕЖНОСТИ И ДОЛГОВЕЧНОСТИ РЕЗЬБОВЫХ СОЕДИНЕНИЙ БУРИЛЬНЫХ ТРУБ

Куанышов Б.А., 2 курс, технологические машины и оборудование, Костанайский региональный университет им. А.Байтурсынова

Нурушев С.З., д.т.н., профессор, Костанайский региональный университет им. А.Байтурсынова

Повышение надежности резьбовых соединений является одной из основных проблем в изделиях машиностроения из-за их широкого применения, универсальности, точности изго-