МРНТИ 20.19.01 DOI 10.48501/8411.2023.98.11.005

Жумадилова М.Б[1]. Орынбасар М.А.[1]
[1]Yessenov University
Қазақстан, Ақтау
e-mail: orinbasar24@gmail.com

МОБИЛЬДІ ҚЫЗМЕТТЕРДЕ РЕСУРСТАР МЕН ДЕРЕКТЕРГЕ ҚОЛ ЖЕТІМДІЛІКТІ ҚАМТАМАСЫЗ ЕТУ ҮШІН ПАЙДАЛАНУҒА БОЛАТЫН АВТОРИЗАЦИЯНЫҢ ТҮРЛЕРІ

Аннотация

Мобильді қызметтердегі ресурстар мен деректерге қауіпсіз және бақыланатын түрде қол жеткізу қазіргі әлемдегі ең маңызды қажеттіліктердің бірі болып табылады. Ақпараттық технологиялардың үнемі дамуы олардың адамның күнделікті өміріне енуіне ықпал етеді, бірақ бөгде адамдар мен шабуылдаушылардан маңызды және жеке деректерге қол жеткізуді шектеу қажет. Авторизация пайдаланушының ақпараттық жүйеге кіру жолындағы алғашқы қадамы болып табылады. Бұл мақалада авторизацияның кең таралған және перспективалы түрлерін салыстырмалы зерттеу ұсынылған, атап айтқанда: есім пен парольге негізделген қол жетімділік, OAuth протоколы, JSON Web Tokens (JWT), API кілттері, биометриялық авторизация. Зерттеуде әдіске шолу, оның артықшылықтары мен кемшіліктері, сондай-ақ пайдалану шаралары мен қолдану аясы қарастырылған.

Кілт сөздер: авторизация, қолжетімділік, OAuth, JWT, API, биометрия, мобильді қызмет.

Жумадилова М.Б[1]. Орынбасар М.А.[1]
[1]Yessenov University
Қазақстан, Ақтау
e-mail: orinbasar24@gmail.com

Типы авторизации, которые можно использовать для обеспечения доступа к ресурсам и данным в мобильных сервисах

Аннотация

Безопасный и контролируемый доступ к ресурсам и данным в мобильных сервисах является одной из самых важных потребностей в современном мире. Постоянное развитие информационных технологий способствует их проникновению в повседневную жизнь человека, но необходимо ограничить доступ к важным и личным данным от посторонних и злоумышленников. Авторизация-это первый шаг пользователя к входу в информационную систему. В данной статье представлено сравнительное исследование наиболее распространенных и перспективных форм авторизации, а именно: доступ на основе имени и пароля, протокол OAuth, JSON Web Tokens (JWT), ключи API, биометрическая авторизация. В исследовании рассмотрен обзор метода, его преимущества и недостатки, а также меры и область применения.

Ключевые слова: авторизация, доступность, OAuth, JWT, API, биометрия, мобильный сервис.

Zhumadilova M.B.[1], Orinbasar M.A.[1]
[1]Yessenov University
Kazakhstan, Aktau
e-mail: orinbasar24@gmail.com

Authorization types that can ve used to provide access tp resources and data in mobile services

Annotation

Secure and controlled access to resources and data in mobile services is one of the most important needs in the modern world. The constant development of information technologies contributes to their penetration into the daily life of a person, but it is necessary to restrict access to important and personal data from outsiders and intruders. Authorization is the first step of the user to log into the information system. This article presents a comparative study of the most common and promising forms of authorization, namely: username and password-based access, OAuth protocol, JSON Web Tokens (JWT), API keys, biometric authorization. The study provides an overview of the method, its advantages and disadvantages, as well as measures and scope of application.

Keywords: authorization, accessibility, OAuth, JWT, API, biometrics, mobile service.

Авторизация – ақпараттық жүйеге қол жеткізуді қамтамасыз ету кезінде пайдаланушыларды немесе жүйелерді сәйкестендіруді қамтамасыз ететін бағдарламалаудағы негізгі механизм. Бұл бағдарламалық жасақтаманы деректерге рұқсатсыз қол жеткізуден қорғаудың бірінші желісі, ол шектеулі пайдаланушы ақпараты болсын немесе әкімшінің жүйенің ішкі бөліктеріне толық қол жетімділігі болсын. Бұл мақалада авторизацияның белгілі түрлеріне, олардың күшті және әлсіз жақтарына, нұсқаларына және қолданудың орындылығына қысқаша талдау келтірілген. Бұл зерттеу архитектуралық шешімді қалыптастыруда және бағдарламалық интерфейсті жүзеге асыруда теңдестірілген шешім қабылдауға көмектеседі. Авторизация түрлерін бағалау қауіпсіздік, масштабталу, іске асыру жаңалықтары, құны, пайдаланушы тәжірибесі және нақты жағдайларда өзгергіштік критерийлері бойынша жүргізілді.

Зерттеудің мақсаты – Мобильді қызметтерде ресурстар мен деректерге қол жетімділікті қамтамасыз ету үшін пайдалануға болатын авторизация түрлерінің ұтымдысын анықтау.

Авторизацияның ең көп таралған әдісі –пайдаланушы аты мен құпия сөзді пайдалану. Бұл әдісте пайдаланушы жүйеге тіркелу кезінде оған бірегей есептік жазба атауын енгізіп, кіру үшін парольді ойластыру керек. Көп жағдайда атау мен рөл қосымшаның немесе сервердің дерекқорында сақталады және кірген кезде пайдаланушы енгізген деректермен салыстырылады [1].

Пайдаланушы аты мен пароль бойынша авторизация берілген деректерді сақталған мәндермен салыстырудың таңдалған принципіне байланысты. Әдетте парольдер бастапқы парольде хэш функцияларын қолданудан алынған хэш мәндері ретінде сақталады. Ал аутентификация процесінде пайдаланушы енгізген деректерді сол алгоритм өңдейді, содан кейін хэш мәндерін салыстырады.

Қауіпсіздікті жақсарту үшін әзірлеушілер bcrypt, Argon2 немесе PBKDF2 сияқты күшті парольді хэштеу алгоритмдерін қолданады [2]. Бұл алгоритмдер қосымша қорғаныс деңгейлерін ұсынады, бұл парольдерді бұзуды есептеуді қымбатқа түсіреді. Хэштеу алгоритмін таңдау парольдің төзімділігіне немесе рұқсат етілмеген деңгейге жетудің басқа техникасына айтарлықтай әсер етеді.

Аты мен құпия сөзіне қол жеткізу қарапайым, барлық жерде кездесетін және пайдаланушыларға ең таныс әдіс. Үшінші тарап кітапханалары мен өнімдерін пайдаланбай кез келген бағдарламалау тілінде жазылған кез келген бағдарламалық платформаға оңай біріктіруге болады. Алайда, оның кемшіліктері бар, мысалы, әлсіз парольдердің осалдығы, белгілі сөз тіркестерінен қарапайым шамадан тыс сәйкестікті таңдауға мүмкіндік береді, пайдаланушының әртүрлі жүйелерде бір парольді қайта қолдануы шабуылдаушыларға қауіпсіздікті оңай бұзуына әкеп соғады. Көбінесе шабуылдаушылар фишингтік шабуылдар арқылы пайдаланушылардың тіркелгі деректеріне қол жеткізе алады. Сондай-ақ, пайдаланушы құпия сөздерінің дерекқорлары хакерлік шабуылдардың негізгі мақсаттарының бірі екенін атап өткен жөн [3,4].

Мобильді жүйеде сәтті тіркелу немесе авторизация кезінде пайдаланушы белгілі бір функционалдылыққа өтетінқ белгіні алады. Әрі қарай, бұл серверге әр сұрауда, әдетте HTTP сұрауының тақырыбында жіберіледі. Сервер өз кезегінде таңбалауышты тексереді және таңбалауыштың жарамдылығын сәтті растау жағдайында сұралған ресурсқа қол жеткізуді қамтамасыз етеді.

Таңбалауышқа негізделген авторизацияны жүзеге асыру кезінде OAuth немесе JSON Web Tokens (JWT) сияқты дайын құрылымдар мен хаттамалар жиі қолданылады. Мұндай шешімдер токсиндерді шығарудың, валидациялаудың және жоюдың стандартталған әдістерін ұсынады, әр түрлі жүйелерде біртұтас тәсіл мен интероперабельділікті қамтамасыз етеді.

OAuth қауіпсіз авторизация үшін бағдарламалауда кең таралған ашық стандарт болып табылады. Ол үшінші тарапқа логин мен пароль жібермей,

пайдаланушы атынан қорғалған ресурстарға шектеулі қол жетімділікті қамтамасыз етеді. OAuth үшінші тараптың қатысуымен интеграцияларға қауіпсіз қол жеткізуді қамтамасыз етуге мүмкіндік береді [5].

OAuth бірнеше нысандарды қамтиды: қайта өңдеу сервері, клиенттік бағдарлама және авторизация сервері (нысаны). Хаттама бірқатар авторизациялық ағындармен жұмыс істейді: растау коды бар ағын, клиенттің толық ағыны, жасырын кіру ағыны, токен жаңарту ағыны және басқалар.

Растау кодының ағынында клиенттік бағдарлама пайдаланушыны авторизация серверіне бағыттайды, онда пайдаланушыдан сұрауды орындау үшін аутентификация және рұқсаттарды растау сұралады. Осыдан кейін авторизация сервері клиентке авторизация сервері арқылы кіру белгісіне айырбасталатын авторизация кодын ұсынады. Осыдан кейін мобильді қызметтегі ресрусты пайдалануға мүмкіндік беріледі.

OAuth көптеген артықшылықтарға байланысты интернет желісіндегі ең көп таралған авторизация протоколдарының бірі болып табылады:

- OAuth веб-беттер, API, мобильді және жұмыс үстелі қолданбалары үшін пайдаланылуы мүмкін.
- авторизация процесінен басқа, OAuth аутентификацияны, жаңартуды және таңбалауыштарды қайтарып алуды икемді конфигурациялауға мүмкіндік береді.
- қауіпсіздікті арттыру. Кіру таңбалауыштары әр сұраныс бойынша пайдаланушының тіркелгі деректерін беру қажеттілігін жояды, бұл тосқауыл қою және рұқсат етілмеген кіру қаупін айтарлықтай азайтады.
- масштабтау. Авторизацияның бұл әдісін мобильді қызметтерде оңай қолдануға болады, бұл мұндай жүйелерді таратылған архитектураға және әртүрлі клиенттердің бағдарламалық жасақтамаға қол жетімділігіне қолайлы етеді.
- пайдаланушы тәжірибесі. Авторизациядан кейін пайдаланушы жүйемен өзара әрекеттесе алады, мобильді қызметтердегі ресурстар мен деректерге қол жеткізеді.

Алайда бірқатар кемшіліктер бар:

- әзірлеуші түсінуі керек көптеген механизмдердің болуына байланысты іске асырудың күрделілігі.
- авторизацияны жүзеге асыратын көптеген сервистері бар таратылған архитектурада жүйенің барлық бөліктерінің сұрауларын өңдеу бойынша аутентификация серверіне үлкен жүктеме түседі. Бұл сервер қандай да бір себептермен істен шыққан жағдайда, қалған қосымшалар дұрыс жұмыс істей алмайды.

Мобильді жүйедегі авторизацияның тағы бір түрі – JSON Web Tokens. JSON Web Tokens (JWT) бағдарламалауда қауіпсіз авторизация әдісі ретінде айтарлықтай танымал болды. Мұндай таңбалауыштар JSON спецификациясының талаптарына сәйкес жасалған автономдық кодтар болып табылады және пайдаланушы идентификаторы мен авторизация ақпаратын көрсетеді. Мұндай қызмет серверге мәліметтер базасына жүгінбестен токендерді тексеруге және аутентификациялауға мүмкіндік береді [6].

JSON Web Token үш бөліктен тұрады: тақырып, пайдалы жүктеме және қолтаңба. Тақырыпта қол қою үшін қолданылатын алгоритм сияқты метадеректер туралы ақпарат бар. Пайдалы жүктемеде пайдаланушы идентификаторын, авторизация аймағын және басқа да байланысты ақпаратты қамтуы мүмкін деректер бар. Қол қою құпия немесе ашық кілт және тақырыпта көрсетілген алгоритм арқылы ақпаратты кодтауды жүзеге асырады.

Аутентификация кезінде сервер қолтаңбаны тексереді, ол қолдан жасалмағанын растайды. Әрі қарай, сервер пайдалы жүктемеден қосымша ақпарат алып, оны авторизациялау және кіруді басқару үшін қолдана алады.

JWT-дің OAuth-қа ұқсас артықшылықтары бар, олар қауіпті емес, масштабталатын және пайдаланушы тәжірибесі бар, сонымен бірге келесі артықшылықтарын ұсына алады:

- автономия. Бұл тәсіл сервер жағында мәліметтер базасын пайдалану қажеттілігін жояды, бұл жүйені одан да ыңғайлы масштабтауға және қосымша сұраныстардың болмауына байланысты өнімділікті арттыруға мүмкіндік береді.
- пайдаланудың қарапайымдылығы және үйлесімділігі. JWT қарапайым іске асыру механизмін ұсынады және әртүрлі бағдарламалау тілдерінде және фреймворктарда жүзеге асырылуы мүмкін ашық стандарттарға негізделген.
- кеңейту. Таңбалауыш пайдалы жүктемені көтере алады, бұл бағдарламашыға авторизацияға қажетті қосымша ақпаратты қосуға мүмкіндік береді.

Алайда бірқатар шектеулер бар:

- таңбалауыш өлшемі. Егер әзірлеуші жүйеге көп мөлшерде ақпарат енгізсе, таңбалауыштың үлкен мөлшерін сатып алуы мүмкін, бұл әр сұраныс бойынша таңбалауыштың тұрақты берілуіне байланысты желінің өнімділігі мен қол жетімділігіне әсер етуі мүмкін. Сондай-ақ, таңбалауыштың ұзындығы тақырыптың HTTP ұзындығымен немесе сервердің қажеттіліктерімен шектелетінін атап өткен жөн.
- ұзақ жұмыс жасайтын токенге нұқсан келтіргенде, оны қайтарып алу өте қиын, өйткені JWT мұндай механизмді қабылдамайды. Таңбалауыштың болуы неғұрлым қысқа болса, жүйенің осалдық терезесі соғұрлым аз болады, бірақ таңбалауышты жаңарту соғұрлым жиі қажет болуы мүмкін.

Авторизацияның кең танылған тағы бір түрі – API кілттері. Бағдарламалық жасақтама интерфейсінің (API) кілттері веб-қызметтер мен API-ге авторизацияланған және рұқсат етілген қол жетімділікті қамтамасыз ету үшін бағдарламалауда кеңінен қолданылады. API кілті – бұл кілт тіркелген қолданба ресурстарына қол жеткізуге мүмкіндік беретін бірегей идентификатор немесе токен. Ол қоңырау шалушы қолданбаны немесе пайдаланушыны авторизациялау үшін әзірлеуші API сұрауына енгізетін тіркелгі деректері ретінде пайдаланылады.

Мұндай авториазация процесі әдетте келесі қадамдар бойынша жүзеге асырылады:

- Кілт жасау. Бұл қадам сервер жағындағы бірегей кілтті шығарады және баспагердің API интерфейсіне кіруді қажет ететін үшінші тарап қолданбасының әзірлеушісіне беріледі. Кілттерді қолмен немесе әзірлеушілерге арналған арнайы автоматтандырылған портал арқылы немесе сол платформаның API көмегімен жасауға болады.
- үй-жай сұранысы. Қолданылатын бағдарламалық интерфейстің сипаттамасына байланысты кілт сұрау жолында, тақырыпта немесе сұрау денесінде параметр ретінде берілуі мүмкін.
- сервер жағында тексеру. Сервер сұранысты алғаннан кейін берілген кілтті тексеруді бастайды. Рұқсат етілген кілттер базасында кілттің болуын тексеру жүргізіледі және осы кілтке берілген рұқсаттар тексеріледі. Егер кілт танылса және рұқсат етілсе, сервер қабылданған сұранысты орындайды.

API кілттерінің келесідей артықшылықтары бар:

- аутентификация механизмінің қарапайымдылығы мен түзулігі. Кілттерді шығару, тұтынушыларға жеткізу және сұрауларға қосу оңай.
- жүйені оңай масштабтауға мүмкіндік береді, өйткені бұл кілттер күрделі басқару механизмін құруды қажет етпестен көптеген пайдаланушылар үшін қолданыла алады.
- жүйеге қол жеткізу құқықтары мен деңгейлерінің нақты кілтін беру арқылы жүзеге асырылатын кіруді егжей-тегжейлі басқару сұраныс кезінде қол жетімді ресурстарға немесе функционалдылыққа қол жеткізуді мұқият бақылауға мүмкіндік береді [7].

Алайда, бұл тәсілдің айтарлықтай кемшіліктері бар, олар негізінен токендердің тұрақтылығы мен ұзақ өмір сүруіне байланысты:

- байланыс арнасын қосымша қорғау қажеттілігі. Кілттерді HTTPS сияқты қорғалған қосылым арқылы беру керек.
- шектеулі қауіпсіздік. Тек API кілттерін пайдалану жетілдірілген шабуылдарға қарсы жүйенің жеткілікті қауіпсіз деңгейіне кепілдік бере алмайды. API кілттерін басқа тәсілдермен, мысалы, берілетін ақпаратты кодтау немесе қосымша авторизация факторлары арқылы біріктіріп аутентификациялау ұсынылады.
- кілттерді дұрыс басқару қажеттілігі. Кілттерді қауіпсіз сақтаудан басқа, бұзылған таңбалауыштарды уақтылы қадағалау және оларды бұғаттау немесе қайта шығару қажет.

Сертификаттарға негізделген авторизация. Авторизацияның бұл түрі сандық сертификаттарға негізделген криптографиялық әдіс болып табылады. Негізінен бұл әдіс жүйенің бөліктері арасында қорғалған байланыс пен өзара сенімді қажет ететін бағдарламаларда қолданылады. Сертификатқа негізделген авторизация пайдаланушыларды немесе жүйелерді сәйкестендіру үшін куәландырушы орталық шығарған ашық кілттер инфрақұрылымын (АКИ) және сенімді сертификаттарды пайдалануды қамтиды. Көбінесе сертификат үшін X.509 формасы қолданылады, оған сәйкес сертификатта сериялық нөмір, тақырып, қол қою алгоритмі, хэш функциясының алгоритмі, жарамдылық мерзімі, ашық кілт және басқа ақпарат болуы керек [8]. Авторизацияның бұл түрімен жұмыс істеу үшін кем дегенде үш элемент болуы керек: клиент, сервер және процестің екі қатысушысына арналған куәлік.

АКИ-те авторизация процесін келесі қадамдарға бөлуге болады:

- сертификат құру. Пайдаланушылар немесе субъектілер жұп криптографиялық кілттерді (жалпыға ортақ және жеке кілттер) және сертификат (CSR) сұрауын жасайды. Содан кейін CSR сертификаттың өзін шығару үшін сенімді қызмет көрсету орталығына жібереді.
- сертификат шығару. Сертификаттау орталығы сұрау салушының бастамашысын анықтайды және CSR-ге қол қояды, ақпараттың түпнұсқалығын бақылау үшін жалпыға ортақ кілт бекітілген цифрлық сертификат жасайды. Сертификат куәландырушы орталықтың цифрлық қолтаңбасымен бекітілген пайдаланушының деректерін және оның ашық кілтін ұсынады. Шығарылғаннан кейін сертификат бастамашыға қайтарылады.
- сертификат беру және тексеру. Авторизация кезінде жүйенің тұтынушысы қол жеткізетін серверге сандық сертификат береді. Сервер куәландырушы орталықтың жария кілтін біле отырып, цифрлық қолтаңбаны алып тастайды және оның хэшін деректер хэшімен тексереді, олардың шынайылығы мен тұтастығына көз жеткізеді және тексеру негізінде сертификаттың дұрыстығы туралы шешім қабылдайды.
- деректерді тексеру. Сервер сертификаттағы клиенттің жалпыға ортақ кілтін пайдаланып, жіберілген деректерді тексереді және сұранысты орындайды.
- өзара аутентификация кезінде екінші тарап ұқсас әрекеттерді орындайды.

Артықшылықтарға мыналар жатады:

криптографиялық механизмдерге негізделген қатаң авторизация. Сандық сертификаттарды пайдалану процестің сенімділігін арттырады.

екі тарап бір-бірін тексере алатын өзара аутентификацияны қолдау, бұл байланыс арнасына деген сенімді одан әрі арттырады.

масштабтау және орталықтандырылған басқару. Ашық кілттер инфрақұрылымын дұрыс пайдалану кезінде сертификаттардағы авторизация көптеген пайдаланушылар үшін бейімделуі мүмкін. Орталықтандырылған басқару сертификаттарды басқару мен қайтарып алу процесін жеңілдетеді.

Алайда, бұл тәсілде бірқатар маңызды шектеулер мен кемшіліктер бар екенін ескеруі керек:

- көптеген сертификаттарды басқару сақтау процесін күрделі

конфигурациялауды, әрекет ету уақытын бақылауды, жаңартуды, сертификаттарды қайта шығаруды талап етеді, ол үшін қосымша құралдар қажет болуы мүмкін. Сондай-ақ, АКИ ұйымдастыру және криптография әдістері туралы білім қажет.

- куәландырушы орталықтарға тәуелділік сертификаттар шығаратын ұйымдардың тиісті мониторингін талап етеді.
- сертификаттарды алу және уақтылы жаңарту қажеттілігіне байланысты пайдаланушы үшін күрделіліктің жоғарылауы.

Қазіргі таңда мобильді жүйелердең кең таралған авторизация түрі – биометриялық авторизация. Биометриялық авторизация адамның бірегей физикалық ерекшеліктерін пайдаланады. Бұл әдіс пайдаланудағы ыңғайлылық пен қауіпсіздіктің арқасында танымал болды. Саусақ іздері, бет ерекшеліктері, дауыс сипаттамалары сияқты биометриялық деректерді көптеген қосымшаларда авторизация үшін пайдалануға болады.

Биометриялық авторизация процесін үш қадамға бөлуге болады:

- тіркеу. Пайдаланушы биометриялық сенсорлар мен құрылғыларды қолдана отырып, өзінің бірыңғай деректерін тіркейді. Бұл ақпарат дерекқорға қорғалған түрде сақталады немесе пайдаланушы тіркелгісінің таңбалауышымен байланысады [9].
- тексеру. Аутентификация кезінде пайдаланушы сканерлеу арқылы биометриялық үлгіні ұсынады, содан кейін жүйе белгілі бір алгоритмдер бойынша енгізілген ақпаратты бұрыннан бар ақпаратпен салыстырады.
- шешім және қол жетімділікті қамтамасыз ету. Салыстыру нәтижелеріне сүйене отырып, жүйе деректердің сақталған мәліметтермен қаншалықты дәл сәйкес келетінін анықтайды. Егер сәйкестік берілген пайыздан асып кетсе, онда жүйе пайдаланушыны тексереді.

Негізгі артықшылықтары:

- қауіпсіздікті арттыру. Биометриялық авторизация пайдаланушыны анықтау процесіне қосымша қауіпсіздік қабатын қосады.
- пайдаланушының ыңғайлылығы. Осы тәсілді қолдана отырып, пайдаланушы бұдан былай тіркелгі деректерін немесе кіру кодтарын есте сақтаудың қажеті жоқ, бұл пайдаланушы тәжірибесінің қолайлылығын арттырады және құпия сөзді таңдаумен байланысты осалдықтар қаупін азайтады.

Алайда бірқатар маңызды шектеулер бар:

- құпиялылық және деректерді қорғау. Мұндай деректер пайдаланушы үшін өте сезімтал және оларды пайдалану оларды сақтау мен берудің төзімділігі туралы көптеген пікірталастардың тақырыбы болып табылады. Сонымен қатар, мұндай деректер жеке деректерді қорғау туралы заңдардың күшіне енуі мүмкін. Сондықтан, әзірлеушілер мәліметтер базасын пайдалану кезінде және қосымшалар арасында тасымалдау кезінде деректердің жоғары дәрежеде сақталуын қамтамасыз етуі керек.
- құрылғылар мен сенсорлардың әртүрлілігі. Әр түрлі құрылғыларда әр түрлі болуы мүмкін дәлдік, сенімділік, интерфейстер және деректерді өңдеу алгоритмдері. Мұндай шешімдерді біріктіретін бағдарламашылар іске асыру жолында көптеген қиындықтарға тап болуы мүмкін.
- жалған позитивтер, істен шығу және зақымдану жиілігі. Биометриялық жабдық та мінсіз емес және жалған позитивтерге жол беруі мүмкін, бұл қауіпсіздіктің ықтимал қаупі. Сондай-ақ, құрылғылар ақпаратты дұрыс өңдемеуі мүмкін және сыртқы факторларға байланысты, мысалы, бетті сканерлеу кезінде жарықтандыру.

Бұл мақалада мобильді жүйелердің авторизациясының классикалық және перспективалық әдістері қарастырылды. Әр әдістің өзіндік артықшылықтары мен кемшіліктері бар, осыған байланысты ол белгілі бір мәселені шешуге жарамды немесе берілген шарттарда қолданылмауы мүмкін. Қолдану туралы

шешімді әзірлеушілер техникалық тапсырмалар мен ақпараттық қауіпсіздік нұсқауларының талаптарына сүйене отырып қабылдауы керек. Сондай-ақ, кез келген тәсілдің кемшіліктерін мультифакторлық авторизация арқылы өтеуге болатындығын атап өткен жөн [7]. Алайда, аутентификация мен авторизацияның әртүрлі тәсілдерін біріктіру осы жұмыстың тақырыбынан тыс ең жақсы шешімдерді анықтау үшін қосымша зерттеуді қажет етеді.

Ең классикалық және танымал нұсқа – пайдаланушы аты мен парольге қол жеткізу, бірақ сонымен бірге бұл әдістің осалдықтарын шабуылдаушылар көбірек зерттейді. Олар техникалық және психологиялық тіркелгі деректерін алу механизмдерін жақсы біледі. Жүйенің тиісті қауіпсіздігін сақтау үшін парольді мүмкіндігінше жиі өзгерту керек, бұл пайдаланушы тарапынан кейбір әрекеттерді және өзекті парольді есте сақтау қажеттілігін талап етеді.

Ең көп зерттелген және жиі пайдаланылатын нұсқа – биометриялық авторизация. Бұл нұсқа мобильді қызметтерде кеңінен танымал. Алайда желі арқылы өзара әрекеттесу кезінде байланыс арнасының қауіпсіздігіне ерекше назар аудару қажет, әйтпесе әдістің барлық күрделілігі мен сенімділігі барлық мағынаны жоғалтады, өйткені мұндай деректерді беру пайдаланушы аты мен парольді беруден түбегейлі ерекшеленбейді. Бірақ бұл әдіс сенсорларға немесе биометриялық үлгілерге сыртқы әсерлер болған кезде мүлдем қолданылмауы мүмкін. Осыны және биометриялық сенсорлардың болуын ескере отырып, авторизацияның бұл түрін енгізілген деректерде, жеке құрылғыларда және операциялық жүйелерде қолданған жөн.

Осылайша, мобильді қызметтердегі авторизация әдістері егжей-тегжейлі қарастырылып, талданды, оларды пайдалану бойынша ұсыныстар берілді, сонымен қатар әрі қарайғы зерттеулерге жолдамалар ұсынылды.

Әдебиеттер:

1. Almadhoun R., Kadha M., Alhemeiri M., Alshehhi M. and Salah K. A user authentication scheme of IoT devices using blockchain-enabled fog nodes 2018, in Proceedings of the 2018 IEEE // ACS 15th International Conference on Computer Systems and Applications (AICCSA), 2018. Aqaba, Jordan. – pp. 1-8.

2. Lally G and Sgandurra D. Towards a framework for testing the security of IoT devices consistently, in Proceedings of the First International Workshop on ETAA, 2018, Barcelona, Spain, September.

3. Park N. Mutual authentication scheme in secure internet of things technology for comfortable lifestyle, Sensors (Swit- zerland), 2015. – vol. 16. – pp. 1-16.

4. Bradley, J., & Sakimura, N. (2019). OAuth 2.0 Security Best Current Practice. RFC 8252.

5. Housley, R., Polk, W., Ford, W., & Solo, D. (2002). Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. RFC 3280.

6. Jones, M., Bradley, J., & Sakimura, N. (2015). JSON Web Token (JWT). RFC 7519.

7. Perols, J. L., Zimmerman, J. L., & Eining, M. M. (2019). Continuous Authentication Using Behavioral Biometrics: A Review. Journal of Management Information Systems, 36(3), 982-1013.

8. Wiedermann, W., & Hyysalo, J. (2019). Behavioral Biometrics and Continuous Authentication: A Survey.

9. Liang, Y., Samtani, S., Guo, B., and Yu, Z. (2020). Behavioral Biometrics for Continuous Authentication in the Internet of Things Era: An Artificial Intelligence Perspective.

Сведения об авторах

Жумадилова Мереке Бапановна
Должность: К.т.н, доцент, заведующая кафедрой «Компьютерные науки» КГТИУ им. Ш. Есенова
Почтовый адрес: 130000, Республика Казахстан, г.Актау
Сот. тел: +7 (707) 689 33 66
E-mail: mereke.zhumadilova@yu.edu.kz
Zhumadilova Mereke Bapanovna
Position: candidate of technical sciences, associate professor, head of the "Computer Science" department CSUTE named after Sh. Yesenov

Mailing address: 130000, Republic of Kazakhstan, Aktau city
Mob.phone: +7 (707) 689 33 66
E-mail: mereke.zhumadilova@yu.edu.kz

Орынбасар Мақсым Айдарбекұлы
Лауазымы: «Ақпараттық жүйелер» мамандығының магистранты, Yessenov university
Пошталық мекен-жайы: 130000, Қазақстан Республикасы, Ақтау қаласы
Ұялы Тел: +7 (702) 958 03 92
E-mail: orinbasar24@gmail.com
Орынбасар Мақсым Айдарбекұлы
Должность: магистрант специальности «Информационные системы» Yessenov university
Почтовый адрес: 130000, Республика Казахстан, г.Актау
Сот. тел: +7 (702) 958 03 92
E-mail: orinbasar24@gmail.com
Orinbasar M.
Position: master's student of "Information systems" Yessenov university
Mailing address: 130000, Republic of Kazakhstan, Aktau city
E-mail: orinbasar24@gmail.com