ҚАЗАҚСТАН РЕСПУБЛИКАСЫ ҒЫЛЫМ ЖӘНЕ ЖОҒАРЫ БІЛІМ МИНИСТРЛІГІ

«Л.Н. ГУМИЛЕВ АТЫНДАҒЫ ЕУРАЗИЯ ҰЛТТЫҚ УНИВЕРСИТЕТІ» КЕАҚ

Студенттер мен жас ғалымдардың
«ǴYLYM JÁNE BILIM - 2024»
XIX Халықаралық ғылыми конференциясының
БАЯНДАМАЛАР ЖИНАҒЫ

СБОРНИК МАТЕРИАЛОВ
XIX Международной научной конференции
студентов и молодых ученых
«ǴYLYM JÁNE BILIM - 2024»

PROCEEDINGS
of the XIX International Scientific Conference
for students and young scholars
«ǴYLYM JÁNE BILIM - 2024»

2024
Астана

УДК 001
ББК 72
G99

«ǴYLYM JÁNE BILIM – 2024» студенттер мен жас ғалымдардың XIX Халықаралық ғылыми конференциясы = XIX Международная научная конференция студентов и молодых ученых «ǴYLYM JÁNE BILIM – 2024» = The XIX International Scientific Conference for students and young scholars «ǴYLYM JÁNE BILIM – 2024». – Астана: – 7478 б. - қазақша, орысша, ағылшынша.

ISBN 978-601-7697-07-5

Жинаққа студенттердің, магистранттардың, докоранттардың және жас ғалымдардың жаратылыстану-техникалық және гуманитарлық ғылымдардың өзекті мәселелері бойынша баяндамалары енгізілген.

The proceedings are the papers of students, undergraduates, doctoral students and young researchers on topical issues of natural and technical sciences and humanities.

В сборник вошли доклады студентов, магистрантов, докторантов имолодых ученых по актуальным вопросам естественно-технических и гуманитарных наук.

УДК 001
ББК 72
G99

ISBN 978-601-7697-07-5

SQL шабуылында қолданылатын жасыру әдістері [4].

Кибершабуылшылар веб-сайттардағы қауіпсіздік тетіктерін айналып өту үшін әртүрлі жасыру әдістерін пайдаланады. Олардың кейбіреулері төменде талқыланды:

1. Жолдық түсініктеме: Қауіпсіздік механизмдерін айналып өту үшін шабуылдаушылар шабуыл жасалған жолдардың ортасында кірістірілген түсініктемелерді пайдаланады.
2. Таңбаларды кодтау немесе қос кодтау: Кейбір WAF-тер он алтылық кодталған кіріс деректерін декодтайды және шабуылдың алдын алып, оларды сүзеді. Оларды айналып өту үшін кибершабуылдаушылар кіріс деректерін екі рет кодтай алады.
3. Регистрді ауыстыру: Кейбір қолданбалар кіші әріппен жазылған SQL кілт сөздерін блоктайды. Осындай жағдайда кибершабуылшылар осы қорғау механизмін айналып өту үшін айнымалы регистрде жазылған кодты пайдаланады. Кейбір желіаралық қалқандарда тұрақты өрнек сүзгісі (regex)/union\select/g бар. Сондықтан олар кіші әріптермен жазылған күдікті кодты сүзе алады.

Білім беру порталдарды киберқауіптерден қорғау үшін келесі шараларды қабылдау қажет:

- Қызметкерлер мен студенттерді оқыту: қызметкерлер мен студенттер үшін киберқауіпсіздік бойынша оқыту бағдарламаларын жүйелі түрде жүргізу маңызды. Олар әртүрлі шабуыл түрлерін және олардан қалай қорғану керектігін білуі қажет.
- Заманауи қауіпсіздік жүйелерін пайдалану: антивирустық бағдарламаларды, желіаралық қалқандарды, шабуылдарды анықтау жүйелерін және басқа қауіпсіздік шараларын орнату шабуылдардың алдын алуға көмектеседі.
- Қатаң қауіпсіздік саясаттарын жасау: білім беру мекемелері қол жеткізуді басқару, құпия сөздер, деректердің сақтық көшірмесін жасау және ақпаратты ортақ пайдалану бойынша қатаң саясаттарды әзірлеуі және енгізуі керек.

Білім беру саласы әрқашанда маңызды аспектілердің бірі екенінін біле отырып, оның қауіпсіздігін қамтамасыз етуді де басты мақсат ретінде қараумыз қажет. Білім беру саласындағы киберқауіпсіздікті қамтамасыз ету қызметкерлер мен студенттерді оқытудан бастап заманауи технологиялық шешімдерді енгізуге дейінгі шараларды біріктіруді талап етеді. Білім беру ұйымдарында қауіпсіздікті сақтау деректердің құпиялылығын қорғап қана қоймай, білім беру процесінің үздіксіздігін қамтамасыз етеді.

Пайдаланылған әдебиеттер тізімі

1. Yousif Yaseen, K. A. (2022). Digital Education: The Cybersecurity Challenges in the Online Classroom (2019-2020). Asian Journal of Computer Science and Technology, 11(2), 33–38. https://doi.org/10.51983/ajcst-2022.11.2.3450

2. Юсиф Ясин, К. А. (2022). Важность кибербезопасности в секторе высшего образования 2022. Азиатский журнал компьютерных наук и технологий, 11 (2), 20–24. https://doi.org/10.51983/ajcst-2022.11.2.3448

3. Қазақстандық білім беру порталдарының рейтингі https://zero.kz/cat_id_7-obrazovanie-nauka/?ysclid=lu5614cmt1913585664

4. Digital Forensics Essentials. EC-Council official curricula. EC-Council, 2021

УДК 512.647

АУТЕНТИФИКАЦИЯНЫ КҮШЕЙТУДЕГІ ИННОВАЦИЯЛЫҚ ТӘСІЛДЕР

Хамитов Алмат Рустемович

almat1001@mail.ru

Л.Н.Гумилев атындағы ЕҰУ Ақпараттық технологиялар факультеті «7М06306 – Ақпараттық қауіпсіздік жүйелері» білім беру бағдарламасының 1-курс магистранты**,** Астана, Қазақстан

Ғылыми жетекшісі – Ташенова Ж.М.

Аннотация. Бұл мақалада цифрлық ортада аутентификацияны күшейтудің қазіргі инновациялық тәсілдері талқыланады. Пайдаланушылардың құпия ақпаратының қауіпсіздігі мен қорғалуын арттыруға бағытталған соңғы технологиялар қарастырылған. Биометрияға, көп факторлы аутентификацияға, алаяқтықты анықтау және алдын алу үшін жасанды интеллектті пайдалануға ерекше көңіл бөлінеді. Әрбір тәсілдің артықшылықтары мен шектеулері, сондай-ақ олардың болашақта ақпараттық қауіпсіздікті дамытуға ықтимал әсері талданады. Зерттеу нәтижелері киберқауіпсіздік мамандары үшін де, аутентификация жүйелерін күшейтіп, қауіптерден қорғағысы келетін ұйымдар үшін де пайдалы болуы мүмкін.

Кілттік сөздер: аутентификация, блокчейн, биометриялық жүйелер, идентификатор, киберқауіпсіздік.

Кіріспе. Қазіргі заманғы ақпараттық қауіпсіздік әлемінде қарапайым аутентификация әдістері бұзудың қарапайымдылығы сияқты кемшіліктерге ұшырайды, ал биометриялық аутентификацияның бірегейлігі бар, бірақ деректердің бұзылу қаупі бар. Бұл тұрғыда, блокчейн шынайы транзакциялар журналын қамтамасыз ете отырып, аутентификацияның маңызды элементіне айналады. Дегенмен, тіпті бұл әдіс осалдықтарсыз емес, сондықтан аутентификация процесінің сенімділігі мен қауіпсіздігін қамтамасыз ету үшін техникалық және адами аспектілерді ескеретін инновациялық тәсілдерді әзірлеу қажет.

Қарапайым аутентификация және биометриялық аутентификациялардың артықшылықтары мен кемшіліктері. Заманауи жағдайларда деректердің қорғалмаған байланыс арналары арқылы берілуі ықтимал қауіп төндіреді, өйткені ақпараттық жүйелерде қол жеткізу шабуылдаушыларға елеулі зиян келтіруі мүмкін құнды ақпаратты қамтиды және өңдейді. Сондықтан ақпараттық қауіпсіздікті қамтамасыз ету өзара әрекеттесуге қатысушылардың түпнұсқалығын тексеру үшін аутентификация әдістері мен құралдарын қолдануды талап етеді. Бұл мақалада қарапайым аутентификация әдістері, соның ішінде қарапайым құпия сөздер арқылы аутентификация қарастырылады.

Қарапайым аутентификация қарапайым құпия сөзді тағайындау арқылы жүзеге асырылады. Қарапайым аутентификацияның ең көп тараған мысалдарының бірі қайта пайдалануға болатын құпия сөздің аутентификациясы болып табылады. Дегенмен, қазіргі заманғы қауіпсіздік жүйелері смарт-карталарды, USB таңбалауыштарын, бір реттік немесе графикалық құпия сөздері бар бағдарламалық және аппараттық құралдардың аутентификация жүйелерін пайдалану арқылы аутентификациялау сияқты тиімдірек аутентификация әдістерін көбірек пайдаланады.

Биометриялық аутентификацияның пайдаланушылар үшін ыңғайлы және интуитивті болғанымен, өзіндік қиындықтары бар. Мысалы, саусақ ізі жағдайында аутентификация жүйесін алдайтын «жасанды саусақты» жасауға болады. Сонымен қатар, биометриялық сканерлерді орнату және техникалық қызмет көрсету қымбатқа түседі.

Қазіргі уақытта биометриялық аутентификация әдістері екі классқа бөлінеді:

1) адамның физиологиялық ерекшеліктеріне негізделген, онымен өмір бойы бірге болатын және жоғалтуға, ұрлауға немесе көшіруге болмайтын статикалық әдістер.

Статикалық әдістерге мыналар жатады:

- саусақ ізінің аутентификациясы
- ирис аутентификациясы
- тордың аутентификациясы
- қол геометриясына негізделген аутентификация
- бет термограммасының көмегімен аутентификация

2) адамдардың мінез-құлық ерекшеліктеріне негізделген динамикалық әдістер.

Динамикалық әдістер:

- дауысты аутентификация
- қолжазба аутентификациясы
- пернетақтадағы қолжазба арқылы аутентификация

Биометриялық аутентификацияның кемшіліктері арасында мыналарды атап өтуге болады:

- Үлгі деректер базасын зиянды модификациялау мүмкіндігі.
- Дерекқорды үнемі жаңартып отыруды талап ететін адамдардың биометриялық сипаттамаларының өзгермелілігі (қартаю, жарақаттар, аурулар және т.б.).
- Биометриялық деректер ұрланған немесе бұзылған кезде тұрақты деректер қауіпсіздігіне қауіп төндіреді.
- Ағып кету жағдайында өзгертуге болмайтын бірегей биометриялық сипаттамалар.
- Көптеген биометриялық жүйелердің жоғары құны.

Сондай-ақ, сәйкестендіру үшін биометрика жиі қолданылатынын, ал пайдаланушы құпия сөздері әлі де аутентификация үшін пайдаланылатынын атап өткен жөн.

Аутентификацияның әртүрлі әдістерін (бірнеше парольдер, бір реттік парольдер, графикалық парольдер, PIN кодтар, биометриялық аутентификация) талдау нәтижелерін жақсы түсіну үшін жүйелеуге және кестеде көрсетуге болады.

Қарапайым аутентификация әдістерін талдай отырып, олардың ақпарат қауіпсіздігіне қауіп төндіретін бірқатар кемшіліктері бар екенін ескеру қажет. Құпиялылыққа, қолжетімділікке және жүйе тұтастығына ықтимал шабуылдардың алдын алу үшін құпия сөздерді жасау және сақтау бойынша ең жақсы тәжірибелерді орындап, күштірек аутентификация схемаларын пайдалану керек.

Аутентификация жүйелеріндегі осалдықтар. Блокчейн аутентификация саласында. Құпия сөз және таңбалауыш негізіндегі аутентификация жүйелерінде бес негізгі осалдық бар:

1. Құпия сөздерді анықтауға бағытталған дөрекі күш сияқты клиенттік шабуылдар.
2. Пароль мәтіндерін немесе токендерге кіру кодтарын ұрлауды қамтитын хост шабуылдары.
3. Ақпаратты тыңдау, ұрлау және көшіру, соның ішінде токендерге арналған аппараттық құрылғыларды бұрмалау.
4. Ұрланған құпия сөзді немесе кіру кодын пайдалануды қамтитын жауап шабуылдары.
5. Клиенттік құрылғыларға вирустарды орнату немесе құрылғыны қашықтан ұрлау қаупін тудыратын трояндық аттар.

Биометриялық аутентификация жеке сәйкестендіру мәселесінің табиғи және сенімді шешімін қамтамасыз етеді. Биометриялық идентификаторлар әр адам үшін бірегей, сондықтан оларды манипуляциялау қиынға соғады. Дегенмен, осыған қарамастан, кейбір биометриялық ерекшеліктер өзгеруі мүмкін, мысалы, жасқа байланысты өзгерістерге немесе ауруларға байланысты дауыс өзгеруі мүмкін және адамның сыртқы келбеті де уақыт өте өзгеруі мүмкін.

1-кесте. Статистика бойынша әртүрлі аутентфикация қолданатын адамдар саны

Multifactor Authentication Methods: A Framework for Their Comparison and Selection
DOI: http://dx.doi.org/10.5772/intechopen.89876

Authentication scheme	Interviewees	Survey respondents
Text passwords (TP)	10	40
Graphical passwords (GP)	1	20
Cognitive authentication (CA)	0	10
OTP (tokens)	7	38
Smart cards (SC)	3	24
Mobile-based (MB)	8	31
Biometrics (B)	5	30
Federated single sign-on (FSSO)	4	22
Proxy-based (PB)	1	8
Others	0	2

Survey respondents – сұрастырылған адамдар саны. Interviewees – аутетификация схемасын білетіндер саны.

Статистикаға қарасақ, аутентификация жаңа, инновациялық тәсілдерін көп адам білмейді. Биометриялық идентификация, блокчейн технологиялары әлі дамып жатыр, және қолданушылар үшін белгісіз әрі түсініксіз.

Аутентификация саласында блокчейнді енгізу ақпараттық қауіпсіздікті қамтамасыз етудегі маңызды қадам болып табылады. Блокчейн – блоктар тізбегі, олардың әрқайсысы транзакциялар немесе оқиғалар туралы ақпаратты қамтиды және қауіпсіздік пен деректердің тұтастығының жоғары деңгейіне ие.

Аутентификация процесінде блокчейнді пайдалану сенімділік пен ашықтықты қамтамасыз етеді. Блокчейн арқылы жасалған токенді жалған жасауға немесе өзгертуге болмайды, өйткені деректердегі кез келген өзгеріс бүкіл блокчейнде көрсетіледі. Бұл тәсіл деректерді манипуляциялау мүмкіндігін болдырмайды және жүйе қауіпсіздігіне кепілдік береді. Смарт-карталар және бет-әлпетті тану сияқты қосымша инновациялық әдістерді блокчейн арқылы біріктіруге болады, бұл бірегей және қауіпсіз аутентификация әдістерін жасайды.

Аутентификация процесінде блокчейнді пайдалану жүйе қауіпсіздігін жақсарту үшін жаңа мүмкіндіктер ашады. Көп факторлы аутентификация және басқа инновациялық әдістермен бірге блокчейн деректерді сенімді қорғауды қамтамасыз етеді және киберқауіпсіздік қауіпсіздігіне кепілдік береді.

Қорытынды. Қорытындылай келе, аутентификацияның инновациялық әдістерін енгізу, соның ішінде блокчейнді қолдану қазіргі әлемдегі ақпараттық жүйелердің қауіпсіздігін қамтамасыз ету үшін өте маңызды. Блокчейн қамтамасыз ететін деректер тұтастығы мен процестің ашықтығының жоғары деңгейінің арқасында аутентификация жүйелері сенімдірек және манипуляцияға төзімді болады. Дегенмен, әрбір аутентификация әдісінің артықшылықтары мен шектеулерін, соның ішінде биометриялық және қарапайым аутентификацияны ескеру қажет. Әртүрлі әдістер мен инновацияларды қамтитын кешенді тәсіл ғана деректерді тиімді қорғауды қамтамасыз етеді және ұзақ мерзімді перспективада киберқауіпсіздіктің жоғары деңгейін сақтайды.

Қолданылған әдебиеттер тізімі

1. Мартынова, Л. Е. Исследование и сравнительный анализ методов аутентификации / Л. Е. Мартынова, М. Ю. Умницын, К. Е. Назарова, И. П. Пересыпкин. — Текст : непосредственный // Молодой ученый. — 2016. — № 19 (123). — С. 90-93.

2. Lean Center. "Новые подходы к аутентификации в кибербезопасности." Lean Center, https://lean-center.ru/novye-podhody-k-autentifikaczii-v-kiberbezopasnosti/.

3. Шакер И. Е. Использование биометрической аутентификации и перспективы ее применения в банковской системе России //Экономика. Налоги. Право. – 2016. – №. 5. – С. 83-89.

Velásquez I. et al. Multifactor authentication methods: a framework for their comparison and selection //Computer and Network Security. – 2019. – С. 87.