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

4. Спирос, А., Папутсис, А., Корицас, И., Менгидис, Н., Илиу, С., Кавальерос, Д., ... Және Компатиарис, И. (2022). Киберқауіптер туралы ақпаратты үнемі байыту бағытында: бал құмыралары туралы мәліметтер жиынтығын зерттеу.. https://doi.org/10.1109/csr54599.2022.9850295

5. Суросо, Дж.және Прастя, С. (2020). Жоғары оқу орындарында siem және honeypot бар киберқауіпсіздік жүйесі. Iop Конференция Сериясы Материалтану және Инженерия, 874(1), 012008. https://doi.org/10.1088/1757-899x/874/1/012008

6. Vrable, M., Ma, J., Chen, J., Moore, D., Vandekieft, E., Snoeren, A., ... & Savage, S. (2005). Потемкин виртуалды бал фермасындағы ауқымдылық, адалдық және ұстамдылық. Acm Sigops Операциялық Жүйелеріне Шолу, 39 (5), 148-162. https://doi.org/10.1145/1095809.1095825

7. Вебер, С., Штайн, С., Пилгерманн, М. Және Шрейдер, Т. (2023). Медициналық киберфизикалық жүйелер үшін шабуылдарды анықтау-әдебиеттерге жүйелі шолу. Ieee Қол Жетімділігі, 11, 41796-41815. https://doi.org/10.1109/access.2023.3270225

8. https://www.kaspersky.ru/about/press-releases/2022_klyuchi-dlya-umnyh-ustrojstv-kakie-sochetaniya-loginov-i-parolej-chashe-vsego-vvodyat-zloumyshlenniki

9. https://docs.google.com/forms/d/e/1FAIpQLSfeDQ-6S8_4b7XAtfWvdfpC1BF5F0C524Mw_wtajGsZlPf5Mw/viewform?usp=sharing

ӘОЖ 004.056

ҚАУІПСІЗДІКТІ АРТТЫРУ ӘДІСТЕРІ: КІЛТ ҰЗЫНДЫҒЫН ҰЛҒАЙТУ ЖӘНЕ ХЭШ ФУНКЦИЯЛАРЫН ПАЙДАЛАНУ

Қалыбек Иманғали Рахымжанұлы
imangalikalybek@gmail.com
Л.Н.Гумилев атындағы ЕҰУ, «Ақпараттық қауіпсіздік жүйелері»
білім беру бағдарламасының 1-ші курс магистранты, Астана, Қазақстан
Ғылыми жетекші – Жаркимбекова А.Т.

Аңдатпа. Зерттеу жұмысында криптографиялық қорғаудың екі негізгі аспектісін жақсарту арқылы киберқауіпсіздікті арттыру мәселелері қарастырылады: кілт ұзындығын ұлғайту және хэш функцияларын пайдалану. Үнемі дамып келе жатқан киберқауіптер мен шабуылдаушылардың есептеу қуатының артуы жағдайында авторлар сенімді хэш-функцияларды қолданумен бірге криптографиялық алгоритмдердегі кілт ұзындығын ұлғайтуды ұсынады. Мақалада осы әдістердің тиімділігі талданады және заманауи ақпараттық ортада киберқауіпсіздік деңгейін арттыру үшін оларды қолдану бойынша практикалық ұсыныстар ұсынылады. Зерттеу нәтижесінде осы әдістердің ықтимал қауіптері мен артықшылықтары анықталды, бұл мақаланы ақпараттық қауіпсіздік саласындағы мамандар мен барлық мүдделі тұлғалар үшін өзекті етеді.

Кілт сөздер: ақпараттық қауіпсіздік, шифрлау, криптография, хэш-функция, киберқауіпсіздік, криптографиялық алгоритм.

1. Кіріспе

Қазіргі уақытта цифрлық әлем ақпаратпен тығыз байланысты және желіге қосылған кеңістікті білдіреді. Дегенмен, интернет-технологиялардың өсуімен және цифрлық деректер көлемінің ұлғаюымен киберқауіпсіздік тәуекелдері де артады. Деректер мен жеке ақпаратты қорғаудың тиімді әдістерін қажет ететін ұйымдар мен жеке тұлғаларға технологиялар өзгерген сайын көбірек қауіп төндіреді. Бұл тұрғыда криптография деректердің құпиялылығын, тұтастығын және аутентификациясын қамтамасыз ету құралдарын қамтамасыз ету арқылы негізгі рөл атқарады. Дегенмен, шабуылдың жаңа әдістерінің пайда болуымен және заманауи компьютерлердің есептеу қуатының артуына байланысты бұрын қауіпсіз болып көрінген криптографиялық алгоритмдер уақыт өте келе осал болуы мүмкін. Зерттеу жұмысында біз киберқауіпсіздікті жақсартудың екі маңызды аспектісіне тоқталамыз: кілт ұзындығын ұлғайту

және хэш функцияларын пайдалану. Әдістердің екеуі де деректерді желіде қауіпсіз ұстау және әртүрлі кибершабуылдардан қорғау үшін өте маңызды. Осы зерттеуде аталған әдістердің тиімділігін, олардың ықтимал қауіптері мен артықшылықтарын талдап, оларды бүгінгі цифрлық ортада қолдану бойынша практикалық ұсыныстарды қарастырамыз. Киберқылмыскерлер шабуыл әдістерін үнемі жетілдіретін бүгінгі ақпараттық ландшафтта қауіпсіздік стратегияларын үнемі жаңартып отыру қажет. Кілт ұзындығын ұлғайту және күшті хэш функцияларын пайдалану виртуалды активтер мен жеке құпиялылықты қорғауды қамтамасыз ету үшін маңызды қадамдар болып табылады.

2. Кілт ұзындығын ұлғайту

Криптография – деректерді шифрлау және дешифрлау арқылы қорғау әдістерін жасауға арналған ғылым саласы[1]. Ол ақпараттың құпиялылығы мен тұтастығын қамтамасыз ететін математикалық алгоритмдер мен хаттамаларға негізделген. Криптографияның негізгі аспектілерінің бірі шифрлау процесі болып табылады, ол пайдаланушы оқи алатын ашық мәтінді арнайы кілтсіз оқылмайтын шифрланған мәтінге түрлендіреді. Шифрленген мәтін ашық байланыс арналары бойынша берілуі мүмкін, бірақ бастапқы деректерге сәйкес кілті бар авторизацияланған алушы ғана қол жеткізе алады. Шифрлау әдістері ретінде әртүрлі тәсілдер қолданылады, соның ішінде симметриялық және асимметриялық шифрлау. Симметриялық криптографияда бір кілт хабарламаны шифрлау және шифрын ашу үшін қолданылады. Асимметриялық шифрлау, керісінше, жұп кілттерді пайдаланады: ашық және жабық. Ашық кілт хабарламаларды шифрлау үшін, ал жабық кілт олардың шифрын ашу үшін қолданылады. Кілт ұзындығын ұлғайту шифрлау алгоритмдерінің қауіпсіздігін арттырудың ең кең таралған әдістерінің бірі болып табылады. Кілт ұзындығы ұлғайған сайын ықтимал кілттік кеңістік азаяды, бұл кездейсоқ сәйкестіктерді пайдаланатын шабуылдарды баяулатады. Стивенсон мен Барнетт атап өткендей, кілт ұзындығын 128 биттен 256 битке дейін ұлғайту криптоаналитиктің жұмысын әлдеқайда қиындатады[2]. 1-ші суретте криптографиялық шифрлау алгоритмінің кілт ұзындығына сәйкес комбинациялар саны көрсетілген[3].

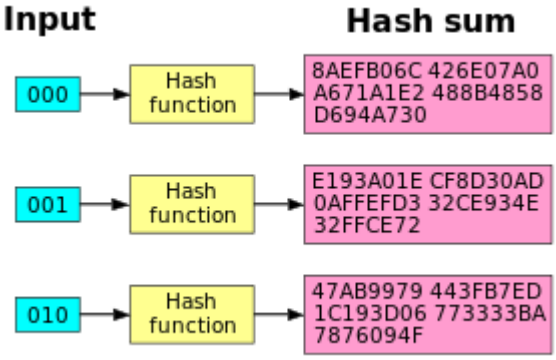
Key Size	Possible combinations
1-bit	2
2-bit	4
4-bit	16
8-bit	256
16-bit	65536
32-bit	4.2×10^{9}
56-bit (DES)	7.2×10^{16}
64-bit	1.8×10^{19}
128-bit (AES)	3.4×10^{38}
192-bit (AES)	6.2×10^{57}
256-bit (AES)	1.1×10^{77}

Сурет 1 Кілт ұзындығына байланысты мүмкін комбинациялар саны

Криптографиядағы кілт ұзындығының маңыздылығын бағаламауға болмайды, өйткені ол жүйенің қауіпсіздік деңгейіне тікелей әсер етеді. Кілт ұзындығы деректерді шифрлау және дешифрлау үшін пайдалануға болатын ықтимал комбинациялардың санын анықтайды. Кілт неғұрлым ұзағырақ болса, соғұрлым көп комбинациялар пайдаланылады, бұл оны бұзуды қиындатады және көбірек уақыт пен ресурстарды қажет етеді. Қазіргі шифрлау жүйелері әдетте ұзындығы бірнеше ондаған немесе жүздеген биттік кілттерді пайдаланады. Мысалы, AES (Advanced Encryption Standard) стандарты 128, 192 немесе 256 биттік кілттерді пайдалана алады.

3. Хэш функцияларын қолдану

Ақпараттық қауіпсіздік саласында деректердің тұтастығын қамтамасыз ету және ақпараттың шынайылығын тексеру үшін хэш функциялары кеңінен қолданылады. Хэш функциясы - еркін ұзындықтағы кіріс деректерін хэш мәні немесе дайджест деп аталатын тұрақты ұзындықтағы жолға түрлендіретін алгоритм. Хэш функциялары деректердің тұтастығын қамтамасыз ететін криптографиядағы маңызды құрал болып табылады және оларды анықтаусыз өзгерту мүмкін емес. Шифрлау алгоритмдерімен бірге хэш функцияларын пайдалану жүйе қауіпсіздігінің жалпы деңгейін арттырады. Фергюсон мен Шуфельттің жұмысына сәйкес, жақсы жобаланған хэш функциялары деректердің тұтастығын қорғауды қамтамасыз етеді[4]. Хэш-функциялардың негізгі қолдануларының бірі нәтижесінде алынған хэш мәнін белгілі дұрыс мәнмен салыстыру арқылы файлдар мен деректердің тұтастығын тексеру болып табылады. Деректерге хэш функцияларын қолдану және алынған хэш мәндерін күтілетін мәндермен салыстыру арқылы тіпті кішкене өзгерістерді де анықтауға болады, бұл оларды жалған немесе өзгертілген файлдарды анықтау үшін пайдалы құрал етеді. Файлдар мен деректердің тұтастығын тексеру үшін хэш функцияларын пайдалану стандартты ақпараттық қауіпсіздік тәжірибесі болып табылады және сақталған ақпаратқа рұқсатсыз өзгертулерді болдырмауға көмектеседі. Бұл әдіс қосымша қорғау деңгейін және қазіргі ақпараттық жүйелердегі деректердің тұтастығына сенімділікті қамтамасыз етеді. Хэш-функциялардағы көшкін эффектісі - бұл кіріс деректеріндегі азғантай өзгерістің өзі шығыс хэш мәнінің айтарлықтай өзгеруін тудыратын құбылыс. Бұл әсер хэш функцияларының қауіпсіздігінің кілті болып табылады және деректерді анықтаусыз өзгертуге әрекеттенетін шабуылдардан қорғау үшін қолданылады. Хэш-функция көшкін әсерінен өткенде, кіріс деректеріндегі кішкене өзгерістердің өзі хэш мәнінің түбегейлі өзгеруіне әкеледі. Бұл шабуылдаушы бастапқы деректерде тек бір битті өзгертсе де, нәтижесінде алынған хэш мәні түпнұсқадан айтарлықтай ерекшеленетінін білдіреді. 2-ші суретте көшкін эффектісіне мысал келтіріілген. Бұл әрекет хэш функцияларын деректер тұтастығын тексеруге және бұрмалауды анықтауға арналған сенімді құралдарға айналдырады.



Сурет 2 Көшкін эффектісі

4. Қауіпсіздікті жақсарту стратегиялары

Әдістерді біріктіру: кілт ұзындығын ұлғайту және хэш функцияларын пайдалану сияқты әртүрлі әдістерді біріктіру қауіпсіздікті жақсартудың тиімді стратегиясы болып табылады. Бұл ықтимал шабуылдарға қосымша кедергілер жасайды және жалпы жүйе қауіпсіздігін күшейтеді.

Тұрақты жаңарту: Жаңа қауіптер мен осалдықтарды ескеру үшін алгоритмдер мен қауіпсіздік параметрлерін жүйелі түрде жаңарту қажет. Хопкинс пен Ли (2019) атап өткендей, бұл қауіпсіздіктің жоғары деңгейін сақтауға және қауіпсіздік тәжірибесінің ескіруіне жол бермеуге көмектеседі [5].

Қызметкерлерді оқыту: Персоналды дұрыс қауіпсіздік тәжірибесіне үйрету ақпараттық қауіпсіздіктің негізгі аспектісі болып табылады. Бұған криптографиялық қауіпсіздіктің соңғы тенденцияларынан хабардар болу және кілттер мен құпия сөздерді сақтаудың қауіпсіз

әдістерін пайдалану кіреді. Бұдан басқа, тиімді қауіпсіздік стратегиясы ықтимал осалдықтарды анықтау және ықтимал қауіптерге жылдам әрекет етуге мүмкіндік беретін қауіпсіздік инциденттерін талдау үшін жүйелі жүйелік аудиттерді де қамтиды. Қауіпсіздік алгоритмдері мен параметрлерін жаңарту және жақсарту - шабуылдың жаңа әдістері мен технологиялық жетістіктерді ескеруі қажет үздіксіз процесс. Персоналдың киберқауіпсіздіктің ағымдағы тенденциялары туралы хабардар болуын жоғары деңгейде ұстау және оларды деректерді қорғаудың заманауи әдістеріне үйрету де ақпараттық қауіпсіздіктің маңызды аспектісі болып табылады. Бұл көбінесе ақпараттық жүйені бұзу тізбегінің бірінші буыны болып табылатын әлеуметтік инженерияны, фишингтік шабуылдарды және әлеуметтік инженерлік шабуылдардың басқа түрлерін болдырмауға көмектеседі. Осылайша, аталған әдістер мен стратегиялардың үйлесімі ақпараттық қауіпсіздікті арттыруға және әртүрлі қауіптерден қорғауға кешенді көзқарасты қамтамасыз етеді.

Қорытынды

Шифрлау алгоритмдерінің қауіпсіздігін қамтамасыз ету қазіргі цифрлық әлемде ақпараттық қауіпсіздік стратегиясының құрамдас бөлігі болып табылады. Қауіпсіздікті жақсартуға кешенді көзқарас, оның ішінде кілт ұзындығын ұлғайту, хэш-функцияларды және басқа стратегияларды пайдалану үнемі дамып отыратын қауіптер мен технологиялар контекстінде қажет.

Кілт ұзындығын ұлғайту криптографиялық жүйелердің беріктігін қамтамасыз етудің негізгі әдістерінің бірі болып табылады. Кілттің ұзындығы неғұрлым ұзақ болса, бұл шифрды бұзуды қиындатады және шабуылдаушылар үшін криптоанализді қиындата түседі. Қысқа кілттерді пайдаланудан ұзағырақ кілттерге көшу қазіргі ақпараттық ортада сенімдірек деректерді қорғауды қамтамасыз етеді.

Ақпараттың тұтастығын қамтамасыз етуде және оның түпнұсқалығын растауда хэш-функцияларды пайдалану да маңызды рөл атқарады. Хэш функциялары алынған хэш мәндерін күтілетін хэш мәндерімен салыстыру арқылы файлдар мен хабарлардың тұтастығын жылдам тексеруге мүмкіндік береді. Көшкін әсерінің арқасында деректердегі шағын өзгерістердің өзі хэш мәндерінің күрт өзгеруіне әкеледі, бұл оларды жалған немесе өзгертілген деректерді анықтаудың тиімді құралына айналдырады.

Дегенмен, шифрлау алгоритмдерінің қауіпсіздігін арттыру тек техникалық әдістерді ғана емес, сонымен қатар ақпараттық қауіпсіздіктің әлеуметтік аспектілеріне назар аударуды талап етеді. Қызметкерлерді қауіпсіздіктің жақсы тәжірибесіне үйрету және оларды киберқауіпсіздіктің соңғы тенденцияларымен жаңартып отыру ұйымдағы ақпараттардың қауіпсіздігін сақтауда маңызды рөл атқарады.

Осылайша, қауіпсіздік техникасын үздіксіз жаңарту және жетілдіру, соның ішінде кілт ұзындығын ұлғайту, хэш функцияларын пайдалану және қызметкерлерді оқыту шифрлау алгоритмдерінің қауіпсіздігін жақсарту стратегиясының маңызды аспектілері болып табылады. Бұл кешенді тәсіл ақпаратты әртүрлі қауіптерден тиімді қорғайды және ұйымдарға жылдам өзгеретін киберқылмыс пен технологиялық қиындықтарға бейімделуге көмектеседі.

Пайдаланылған әдебиеттер тізімі

1. Stallings, W. (2017). Cryptography and Network Security: Principles and Practice (7th Edition). Pearson.

2. Стивенсон, У. және Барнетт, Э. (2016). Кілт ұзындығын ұлғайту: ақпаратты қорғаудың тиімді әдісі. Криптографиялық инженерия журналы, 8(2), 123-135.

3. How safe is AES encryption? | Advanced encryption standard, https://www.kryptall.com/index.php/information/how-safe-is-aes-encryption

4. Фергюсон, Н. және Шуфельт, Б. (2003). Криптографияда хэш-функцияларды қолдану: принциптері мен тәжірибесі. Криптография: теория және практика, 1(2), 67-89.

5. Хопкинс, М. және Ли, С. (2019). Заманауи қауіптер контекстінде криптографиялық әдістерді жаңарту. Компьютер қауіпсіздігі және ақпаратты қорғау, 15(3), 210-225.