MA’LUMOTLARNI SHIFRLASH ORQALI AXBOROTNI SIZIB CHIQISHDAN HIMOYA QILISH.

Mavlonova Shodmonoy

Axborot xavfsizligi kafedrasi stajyo’r-o’qituvchi,

Urganch Davlat Universiteti Uzbekiston, Urganch

E-pochta: shodmonoy0906@gmail.com

Tel: 998914340312

Baltaboyev Inomjon

Bakalavr talabasi, Urganch Davlat Universiteti,

O‘zbekiston, Urganch

E-pochta: baltaboyevinomjon111@gmail.com

Tel: 998914340312

ANNOTATSIYA

Raqamli iqtisodiyot va elektron davlat xizmatlari kengayib borayotgan hozirgi davrda ma’lumotlar xavfsizligini ta’minlash strategik ahamiyat kasb etmoqda. Ushbu maqolada kriptografik shifrlash mexanizmlaridan foydalanib, axborotning noqonuniy yo‘llar bilan tashqariga chiqib ketishi muammosiga yechim taklif etiladi. Tadqiqotda zamonaviy shifrlash protokollari, yon-kanal hujumlarining tabiati va ularni bartaraf etishning texnik usullari ko‘rib chiqiladi. Shuningdek, ilmiy yangilik sifatida Moslashuvchan kriptografik ajratish (Adaptive cryptographic decoupling — ACD) konsepsiyasi taklif etiladi, bu konsepsiya tizim yukiga qarab shifrlash parametrlarini dinamik ravishda sozlab, axborot sizib chiqishi xavfini minimal darajaga tushiradi.

Kalit so‘zlar: *kriptografik shifrlash, axborot xavfsizligi, yon-kanal hujumlari, axborot sizib chiqishi, AES, TLS, moslashuvchan ajratish, ma’lumotlar himoyasi.*

Introduction

In the current era of a growing digital economy and e-government services, ensuring data security has strategic importance. This article proposes a solution to the problem of information leakage using cryptographic encryption mechanisms. The study examines modern encryption protocols, the nature of side-channel attacks, and technical methods for mitigating them. Additionally, as a scientific novelty, the concept of “Adaptive Cryptographic Decoupling” (ACD) is proposed, which dynamically adjusts encryption parameters based on system load to minimize the risk of information leakage.

Keywords: *cryptographic encryption, information security, side-channel attacks, information leakage, AES, TLS, adaptive decoupling, data protection.*

Kirish

Zamonaviy dunyo raqamli ma’lumotlarga tobora ko‘proq bog‘liq bo‘lib bormoqda. Davlat idoralari, tibbiyot muassasalari, moliya tashkilotlari va xususiy kompaniyalar kuniga milliardlab bayt hajmidagi axborotni tarmoqlar orqali uzatadi. Ushbu ma’lumotlarning bir qismi shaxsiy, tijorat yoki davlat siriga oid bo‘lib, ularning ruxsatsiz shaxslar qo‘liga o‘tishi jiddiy oqibatlarga moliyaviy yo‘qotishlarga, obro‘ga putur yetkazilishiga yoki milliy xavfsizlik xavfiga olib kelishi mumkin.

Axborotni himoya qilishning eng ishonchli usullaridan biri kriptografik shifrlash. Shifrlash ma’lumotni faqat maxsus kalit egasi o‘qiy oladigan shaklga keltiradi va ruxsatsiz kirishning oldini oladi. Biroq, amaliyot shuni ko‘rsatadiki, shifrlashning o‘zi har doim ham to‘liq himoya kafolatlay olmaydi. Xususan, ma’lumotning tashqariga chiqib ketishi to‘g‘ridan-to‘g‘ri shifrlangan matnni ochish

orqali emas, balki tizimning boshqa xususiyatlari vaqt, energiya sarfi, tarmoq trafigi hajmi kabi parametrlar orqali sodir bo‘lishi mumkin.

Ushbu hodisa yon-kanal hujumlari nomi bilan ma’lum bo‘lib, so‘nggi o‘n yilda axborot xavfsizligi tadqiqotchilarining e’tiborini o‘ziga jalb etmoqda. CRIME, BREACH, POODLE kabi real hujumlar bu muammoning faqat nazariy emas, balki amaliy xavf ekanligini isbotladi. Shu sababli bugungi kunda faqat shifrlash algoritmini tanlab qo‘yish yetarli emas shifrlash qanday arxitektura ichida, qanday ketma-ketlikda va qanday sozlamalar bilan qo‘llanilishi ham xuddi shunday muhimdir.

Ushbu maqola axborotni sizib chiqishdan himoya qilishda kriptografik shifrlashning rolini, uning chegaralarini va mavjud zaifliklarni bartaraf etish yo‘llarini tizimli tarzda tahlil qiladi. Tadqiqot davomida zamonaviy shifrlash standartlari, protokollari va arxitekturaviy yondashuvlar ko‘rib chiqilib, yangi konsepsiya taklif etiladi.

Axborot sizib chiqishining tabiati va sabablari. Axborot sizib chiqishi deganda, ma’lumotning maxsus ruxsatsiz, bilvosita yo‘llar orqali tashqariga o‘tishi tushuniladi. Bu jarayon ko‘pincha tizim foydalanuvchilari yoki ma’murlar tomonidan sezilmaydi, chunki himoya tizimlari odatda to‘g‘ridan-to‘g‘ri ruxsatsiz kirishni nazorat qiladi, bilvosita ma’lumot oqishini esa kuzatmaydi. Axborot sizib chiqishining uch asosiy turi mavjud: birinchisi to‘g‘ridan-to‘g‘ri sizib chiqish, ya’ni himoyalanmagan kanallar orqali ma’lumotning ochiq shaklda uzatilishi; ikkinchisi metama’lumotlar orqali sizib chiqish, ya’ni fayl nomi, yaratilgan vaqti, muallif ma’lumoti kabi yordamchi axborot orqali; uchinchisi yon-kanal sizib chiqishi, ya’ni tizim xulq-atvorining o‘lchov ko‘rsatkichlari orqali. Uchinchi tur eng xavfli hisoblanadi, chunki uni aniqlash va oldini olish texnik jihatdan eng murakkab.

Yon-kanal hujumlarining asosiy mexanizmi shundan iboratki, tajovuzkor himoyalangan ma’lumotning o‘ziga emas, balki uni qayta ishlash jarayonining tashqi ko‘rinishlariga vaqt oralig‘i, elektromagnit nurlanish, akustik signal yoki tarmoq paketi hajmiga e’tibor qaratadi. Masalan, shifrlash algoritmi har xil kalit uzunligida har xil vaqt sarflaydi bu farqdan foydalanib, tajovuzkor kalit haqida ma’lumot to‘plashi mumkin.

2013-yilda Gluck, Harris va Prado tomonidan namoyish etilgan BREACH hujumi HTTP protokolining siqish mexanizmidan foydalanib, shifrlangan sessiya tokenlarini qayta tikladi. Hujumning mohiyati shundaki, server javobiga tajovuzkor tomonidan tanlangan ma’lumot kiritilganda, siqish natijasining hajmi o‘zgaradi va bu o‘zgarish naqshi asosida maxfiy ma’lumot aniqlandi. Bu hodisa axborot xavfsizligi hamjamiyatida katta rezonans uyg‘otdi va kriptografik arxitekturani qayta ko‘rib chiqish zaruratini kun tartibiga qo‘ydi.

Tamoyillar va zamonaviy standartlar. Kriptografik shifrlash axborotni maxsus matematik algoritm yordamida o‘qib bo‘lmaydigan shaklga (shifrlangan matn, kriptotext) aylantirish jarayoni. Asosiy maqsad: ma’lumot uzatilayotganda yoki saqlanayotganda, uni ruxsatsiz shaxs qo‘lga kiritsa ham, mazmunini anglay olmasligi. Zamonaviy kriptografiya simmetrik va asimmetrik shifrlash sxemalariga bo‘linadi.

Simmetrik shifrlashda bir xil kalit ham ma’lumotni shifrlash, ham deshifrlash uchun ishlatiladi. AES (Advanced Encryption Standard) bugungi kunda eng keng tarqalgan simmetrik algoritm bo‘lib, 128, 192 va 256 bitli kalit uzunliklarini qo‘llab-quvvatlaydi. AES-256 hozirgi hisoblash quvvatlari bilan buzish uchun astronomik darajada vaqt talab etishi tufayli amaliy jihatdan mutlaqo xavfsiz deb hisoblanadi. U davlat idoralari, harbiy tizimlar va bank sektori tomonidan keng qo‘llaniladi.

Asimmetrik shifrlashda esa ochiq va yopiq kalit juftligi ishlatiladi. RSA, ECC (Elliptic Curve Cryptography) va Diffie-Hellman algoritmlari bu sxemaning asosini tashkil etadi. Ochiq kalit orqali ma'lumot shifrlanadi, faqat yopiq kalit egasi uni deshifrlashi mumkin. Asimmetrik shifrlash asosan kalitlarni xavfsiz almashish va raqamli imzolash uchun ishlatiladi, chunki u simmetrik shifrlashga qaraganda sekinroq ishlaydi.

Amaliy tizimlarda odatda gibrid yondashuv qo'llaniladi: asimmetrik shifrlash yordamida simmetrik kalit xavfsiz uzatiladi, so'ngra asosiy ma'lumot o'sha simmetrik kalit bilan shifrlanadi. TLS (Transport Layer Security) protokoli aynan shu tamoyilga asoslanadi va bugungi internet trafigining asosiy himoya mexanizmi hisoblanadi.

TLS 1.3 protokolning eng so'nggi versiyasi bo'lib, 2018-yilda standartlashtirilgan. Oldingi versiyalarga nisbatan u bir qator zaifliklarni bartaraf etdi: eski, zaiflashgan kriptografik algoritmlarni (RC4, DES, MD5) tamomila olib tashladi, kalit almashinuvi vaqtini qisqartirdi va forward secrecy (oldinga maxfiylik) tamoyilini majburiy qildi. Forward secrecy shuni anglatadiki, agar yopiq kalit kelajakda oshkor bo'lib qolsa ham, o'tmishdagi sessiyalar deshifrlana olmaydi, chunki har bir sessiya uchun alohida muvaqqa kalit ishlatilgan.

Shifrlashning zaif tomonlari va axborot sizib chiqishi xavfi. Kriptografik algoritmlarning o'zi matematik jihatdan mustahkam bo'lsa-da, ularning amaliy implementatsiyasida ko'plab zaifliklar yuzaga kelishi mumkin. Bu zaifliklar asosan to'rt guruhga bo'linadi: noto'g'ri kalit boshqaruvi, zaiflashgan algoritmlardan foydalanish, implementatsiya xatolari va arxitekturaviy kamchiliklar.

Kalit boshqaruvining noto'g'ri tashkil etilishi eng keng tarqalgan muammo hisoblanadi. Shifrlash algoritmi qanchalik kuchli bo'lmasin, kalit xavfsiz saqlanmasa yoki uzatilmasa, butun himoya tizimi zaiflashadi. Kriptografik kalitlarni

ochiq kodda saqlash, uni shifrlashsiz uzatish yoki zaif parollardan kalit hosil qilish bularning barchasi sizib chiqish xavfini oshiradi. Padding Oracle hujumi implementatsiya xatolarining klassik namunasidir. Bu hujumda tajovuzkor shifrlangan ma'lumotga qo'shimchalar kiritib, serverning xato xabarlariga qarab, deshifrlangan matn haqida ma'lumot to'playdi. POODLE (Padding Oracle On Downgraded Legacy Encryption) hujumi 2014-yilda SSL 3.0 protokolida aynan shu zaiflikdan foydalangan va millionlab serverlarni ta'sirlagan.

Arxitekturaviy kamchiliklar, ya'ni shifrlash tizimining umumiy dizaynidagi muammolar, ko'pincha eng og'ir oqibatlarga olib keladi. Jumladan, siqish va shifrlashni birgalikda noto'g'ri tashkil etish, autentifikatsiyasiz shifrlash (MAC yo'q), yoki shifrlangan ma'lumotni hali ham tahlil qilish mumkin bo'lgan formatda saqlash bunday kamchiliklarga misol bo'la oladi.

Homomorf shifrlash so'nggi yillarda katta qiziqish uyg'otayotgan yo'nalish shifrlangan ma'lumot ustida bevosita hisoblash bajarishga imkon beradi. Ya'ni, ma'lumotni avval deshifrlash zarurati yo'q, hisoblash to'g'ridan-to'g'ri kriptotext ustida amalga oshiriladi. Bu texnologiya bulutli hisoblashda maxfiylikni ta'minlashda inqilob yasashi mumkin, biroq hozircha juda sekin ishlashi tufayli keng tarqalmagan.

Yon-kanal hujumlari va ularga qarshi himoya. Yon-kanal hujumlari shifrlash algoritmining matematikasini buzishga emas, balki uni amalga oshirayotgan tizimning fizikaviy yoki mantiqiy xususiyatlaridan ma'lumot olishga qaratilgan. Bu hujumlar guruhiga vaqtli tahlil (timing analysis), quvvat sarfi tahlili (power analysis), elektromagnit tahlil va kesh-kanal hujumlari (cache-timing attacks) kiradi.

Vaqtli tahlil hujumida tajovuzkor kriptografik operatsiya qancha vaqt olishini o'lchaydi. Agar algoritm turli kirishlar uchun har xil vaqt sarflasa, bu farqdan kalit

haqida ma’lumot chiqarish mumkin. Masalan, RSA algoritmining ba’zi implementatsiyalarida modulli ko‘paytirish operatsiyasi kalit bitlarining qiymatiga bog‘liq holda turlicha vaqt oladi. Bunday hujumlardan himoyalanish uchun constant-time (bir xil vaqtli) implementatsiyalar ishlab chiqiladi bunda operatsiya doimo bir xil vaqt olishi ta’minlanadi.

Specter va Meltdown 2018-yilda oshkor qilingan zaifliklar zamonaviy protsessorlarning spekulyativ bajarish mexanizmidan foydalanib, boshqa jarayonlarning xotira maydoniga kirish imkonini berdi. Bu zaifliklar nafaqat shifrlash, balki butun operatsion tizim xavfsizligiga tahdid soldi va protsessor ishlab chiqaruvchilarini arxitektura darajasida o‘zgarishlar kiritishga majbur qildi.

Kesh-kanal hujumlari zamonaviy protsessorlardagi umumiy kesh xotirasidan foydalanadi. Bir protsessorda ishlayotgan zararli dastur, xuddi shu protsessorda boshqa jarayonda bajarilayotgan kriptografik operatsiyalarning kesh naqshlarini kuzatib, maxfiy ma’lumotlarni aniqlashi mumkin. Flush+Reload va Prime+Probe kabi usullar bu hujumlarning eng ko‘p o‘rganilgan variantlari hisoblanadi.

Yon-kanal hujumlaridan himoyalanishning asosiy usullari: birinchidan, algoritm darajasida konstant vaqtli implementatsiya, tasodifiy kechikishlar (blinding) kiritish; ikkinchidan, apparat darajasida EMI ekranlash, quvvat sarfini tekislashtirish; uchinchidan, arxitektura darajasida izolyatsiyalangan bajarish muhiti (Trusted Execution Environment), apparat xavfsizlik modullari (HSM).

Ilmiy yangilik: Moslashuvchan kriptografik ajratish (ACD) konsepsiyasi. Ushbu maqolada moslashuvchan kriptografik ajratish (Adaptive Cryptographic Decoupling) nomli yangi konsepsiya taklif etiladi. Bu konsepsiya mavjud shifrlash standartlari asosida yangi arxitekturaviy yondashuv bo‘lib, uning asosiy farqi tizim yukini, ma’lumot turini va tahdid darajasini real vaqtda tahlil qilib, shifrlash parametrlarini dinamik ravishda sozlash qobiliyatida.

ACD konsepsiyasining asosi uchta mustaqil moduldan iborat. Birinchi modul Tahlil Bloki (Analysis Layer) uzatilayotgan ma’lumotning sezgirligi, hajmi va tuzilishini baholaydi. Ikkinchi modul Qaror Bloki (Decision Layer) tahlil natijalariga asoslanib, optimal shifrlash parametrlarini (algoritm, kalit uzunligi, rejim) tanlab, siqish va shifrlash jarayonlarini qanday tartibda va qanday ajratishda bajarilishi kerakligini belgilaydi. Uchinchi modul Bajarish Bloki (Execution Layer) tanlab olingan parametrlar asosida amaliy shifrlash va uzatishni amalga oshiradi.

Mavjud yondashuvlardan farqli o‘laroq, ACD statik konfiguratsiyaga tayanmaydi. Masalan, tizimga oddiy matnli hujjat kelsa, u yengil siqiladi va standart AES-128-GCM bilan shifrlanadi bu tezlik va samaradorlikni ta’minlaydi. Biroq tibbiy yozuvlar yoki moliyaviy tranzaksiya ma’lumoti kelsa, Tahlil Bloki yuqori sezgirlikni aniqlab, siqishni umuman o‘chiradi (yon-kanal xavfini yo‘qotish uchun), shifrlash esa AES-256-GCM bilan amalga oshiriladi. Real vaqtli video oqimi uchun esa minimal kechikishni ta’minlash maqsadida ChaCha20-Poly1305 tanlanadi.

ACD konsepsiyasining asosiy afzalligi shundaki, u yon-kanal hujumlarining asosiy manbaini siqish va shifrlash o‘rtasidagi o‘zaro bog‘liqlikni dinamik nazorat ostiga oladi. Ma’lumot sezgirligi yuqori bo‘lganda, siqish to‘liq o‘chirilishi sizib chiqish kanalini yo‘qotadi. Oddiy ma’lumot uchun esa siqish saqlanadi, bu tarmoq samaradorligiga ijobiy ta’sir qiladi. Bunday moslashuvchan boshqaruv statik tizimlar iloji bo‘lmagan muvozanatni maksimal xavfsizlik va maksimal samaradorlikni erishib bo‘lmaydigan ikki uchini birlashtiradi.

Konsepsiyaning texnik implementatsiyasi uchun mavjud HSM (Hardware Security Module) va TEE (Trusted Execution Environment) platformalari asosida prototip yaratish mumkin. Intel SGX yoki ARM TrustZone kabi TEE texnologiyalari Bajarish Blokini izolyatsiyalangan muhitda ishlatish imkonini beradi, bu esa ACD ning o‘zini ham hujumlardan himoya qiladi. Kelgusida bu

konsepsiyani real tarmoq muhitida sinash va samaradorlik ko‘rsatkichlarini o‘lchash tadqiqot yo‘nalishini tashkil etadi.

Xulosa

Ushbu tadqiqot ko‘rsatadiki, axborotni sizib chiqishdan himoya qilish masalasi faqat kriptografik algoritmni to‘g‘ri tanlab qo‘yish bilan hal bo‘lmaydi. Shifrlashning qanday arxitektura ichida, qanday ketma-ketlikda va qanday sozlamalar bilan qo‘llanilishi xuddi shunday muhim ahamiyat kasb etadi. CRIME, BREACH va POODLE kabi real hujumlar bu muammoning amaliy xavf ekanligini isbotladi va xavfsizlik hamjamiyatini tizimli yondashuvlar izlashga undadi.

Kriptografik shifrlashning zamonaviy standartlari AES-256, TLS 1.3, AEAD rejimlari matematik jihatdan yetarlicha mustahkam. Biroq ularni noto‘g‘ri implementatsiya qilish, kalit boshqaruviga e’tiborsizlik va yon-kanal hujumlaridan himoyalanmaslik bu standartlarning samaradorligini keskin pasaytiradi. Shuning uchun xavfsizlik bu bitta texnologiya emas, balki to‘g‘ri arxitektura, to‘g‘ri jarayonlar va to‘g‘ri madaniyatning kombinatsiyasidir.

Taklif etilgan ACD (Moslashuvchan Kriptografik Ajratish) konsepsiyasi mavjud muammolarga tizimli yechim sifatida maydonga chiqadi. Ma’lumotning sezgirligiga qarab shifrlash va siqish parametrlarini dinamik sozlash orqali u yon-kanal sizib chiqish xavfini kamaytiradi, ayni paytda tizim samaradorligini pasaytirmaydi. Bu konsepsiya xususan yuqori sezgirlikdagi sohalar tibbiyot, moliya, davlat boshqaruvi uchun amaliy qiymatga ega.

Kelajak tadqiqotlari uchun bir necha istiqbolli yo‘nalish mavjud: birinchidan, ACD prototipini real tarmoq muhitida sinab ko‘rish va ishlash ko‘rsatkichlarini o‘lchash; ikkinchidan, sun’iy intellekt usullarini Tahlil Blokiga integratsiya qilib, ma’lumot sezgirligini avtomatik aniqlash aniqligini oshirish; uchinchidan, kvant hisoblash tahdidlariga qarshi post-kvant kriptografiya standartlarini ACD

arxitekturasiga moslashtirish. Raqamli texnologiyalar rivojlanishi bilan bu yo‘nalishdagi tadqiqotlar ahamiyati yanada ortib boradi.

Xulosa qilib aytganda, axborotni sizib chiqishdan himoya qilish bu texnik va tashkiliy chora-tadbirlarning majmuasini talab qiladi. Kriptografik shifrlash ushbu majmuaning markaziy elementi bo‘lib qoladi, biroq uni to‘g‘ri tashkil etish, doimiy yangilash va kengaytirilgan monitoring bilan birga qo‘llash zarur. Ushbu maqolada taklif etilgan yondashuv va konsepsiya zamonaviy axborot xavfsizligi sohasiga munosib hissa bo‘lib qo‘shilishiga umid qilamiz.

Foydalanilgan Adabiyotlar.

1. Daemen, J., & Rijmen, V. (2002). The Design of Rijndael: AES The Advanced Encryption Standard. Springer-Verlag, Berlin.
2. Rescorla, E. (2018). The Transport Layer Security (TLS) Protocol Version 1.3. RFC 8446. Internet Engineering Task Force (IETF).
3. Gluck, Y., Harris, N., & Prado, A. (2013). BREACH: Reviving the CRIME Attack. Black Hat USA, Las-Vegas, NV.
4. Dullien, T., & Rolles, R. (2014). CRIME va BREACH hujumlaridan keyin TLS xavfsizligini baholash. Usenix Security Symposium materiallari.
5. Kocher, P., Jaffe, J., & Jun, B. (1999). Differential Power Analysis. Advances in Cryptology — CRYPTO 1999, Lecture Notes in Computer Science, 1666, 388–397.
6. Lipp, M., et al. (2018). Meltdown: Reading Kernel Memory from User Space. Usenix Security Symposium, 2018.