KRIPTOGRAFIK XAVFSIZLIKNI TA’MINLASHDA QAYBIRI USTUNROQ APPARAT YOKI DASTURIY TA’MINOTGA ASOSLANGAN SHIFRLASH

Allanov Orif Menglimuratovich
TATU, Kiberxavfsizlik va kriminalistika kafedrasi mudiri, phd.
E-mail: orif_allanov@mail.ru

Ahmadov Ulug‘bek Said o‘g‘li
TATU magistranti
E-mail: ahmadovulugbek98@gmail.com

ANNOTATSIYA

Ushbu maqolada kriptografik apparat va dasturiy vositalar va ularning taxlili, amaliyotda qaybiridan foydalanish kerakligi tavsiflangan.

Kalit so‘zlar: kriptografiya, shifrlash, deshifrlash, kriptografik apparat vositalar, kriptografik dasturiy vositalar, xavfsizlik, smart-kartalar

Shifrlash - bu fayllar va xabarlarni kodlash jarayoni bo‘lib,ma’lumotlarni qabul qiluvchidan boshqa hech kim ma’lumotlarga kirishi yoki o‘qishi mumkin emas. U oddiy matnli ma’lumotlarni o‘qib bo‘lmaydigan shifrlangan matnga aylantirish uchun murakkab algoritmlardan foydalanadi, bu faqat vakolatli shaxslar tomonidan kriptografik kalit yordamida dekodlanishi mumkin.Shifrlash ma’lumotlaringizni xavfsiz saqlash uchun juda muhim vositadir. Fayllaringiz shifrlanganda, ularni maxfiy shifrlash kalitisiz butunlay o‘qib bo‘lmaydi. Agar kimdir shifrlangan fayllaringizni o‘g‘irlasa, ular bilan hech narsa qila olmaydi.[5]

Murakkab algoritmlarni buzish qiyinligi ma’lumotlarning yaxlitligi va maxfiyligini himoya qilish uchun kriptografik himoyani juda qimmatli qiladi. Shuning uchun kriptografik himoya ko‘pincha tibbiy yozuvlar, moliyaviy ma’lumotlar, mijozlar ma’lumotlari va mulkiy hujjatlar kabi juda nozik ma’lumotlarni boshqaradigan korxonalar uchun asosiy xavfsizlik chorasi hisoblanadi.

Kriptografik himoyaning ikki turi mavjud: apparatga asoslangan shifrlash va dasturiy ta’minotga asoslangan shifrlash. Ikkalasi ham turli afzalliklarni taklif qiladi. Xo‘sh, bu usullar nima va ular nima uchun muhim?

Dasturiy ta’minotga asoslangan shifrlash

Dasturiy ta’minotga asoslangan shifrlash, nomidan ko‘rinib turibdiki, dasturiy ta’minot yordamida ma’lumotlarni xavfsiz saqlash jarayonidir.Dasturiy ta’minotga asoslangan shifrlash ma’lumotlarni shifrlash uchun kompyuterning qayta ishlash

quvvatidan foydalanadigan dasturlarni anglatadi. Ushbu turdagi shifrlash odatda foydalanuvchilarni autentifikatsiya qilish uchun shifrlash kalitlari sifatida parollarga tayanadi.Bu kichik kompaniyalar uchun tejamkor usul hisoblanadi.Biroq ushbu usulda shifrlash dasturi va boshqa dasturlar ham bitta protsessorda ishlagani sababli,ushbu usul kompyuter ishlash jarayonini sezilarli darajada sekinlashtiradi.[2]

Axcrypt, BitLocker, FileVault, VeraCrypt, DiskCryptor va boshqalar qimmatli ma’lumotlarni xavfsiz saqlash uchun foydalanishga eng yaxshi dasturiy shifrlash vositalaridir.

Shifrlash dasturining ajoyib jihati shundaki, u deyarli har qanday biznes yoki sanoat uchun ochiqdir. Ko‘pgina shifrlash dasturiy echimlari asosiy operatsion tizimlar (OT) va qurilmalar bilan mos keladi, shuning uchun kam konfiguratsiya talab qilinadi. Shifrlash dasturi har qanday dastur kabi ishlaydi, bu sizga xatolarni tuzatish va xususiyatlarni yangilash uchun yangilanishlarni o‘rnatish imkonini beradi. Bundan tashqari, shifrlash dasturi juda tejamkor xavfsizlik chorasidir. Aslida, Bitlocker va FileVault kabi kuchli shifrlash vositalari zamonaviy Windows va Mac kompyuterlarida bepul o‘rnatilgan. Bundan tashqari, dasturiy ta’minot kompaniyangiz bo‘ylab osongina tarqatilishi mumkin va sizdan qo‘shimcha apparat sotib olishingizni talab qilmaydi.[1]

Apparatga asoslangan shifrlash

Apparatga asoslangan shifrlash foydalanuvchilarni autentifikatsiya qilish va ma’lumotlarni shifrlash uchun maxsus ishlab chiqilgan protsessorli qurilmadan foydalanadi. Apparat shifrlash qurilmalariga shifrlangan USB va tashqi qattiq disklar, o‘z-o‘zini shifrlovchi disklar, SSD-lar va hatto o‘rnatilgan shifrlash qobiliyatiga ega mobil telefonlar misol bo‘ladi. Parollarni shifrlash kalitlari sifatida ishlatiladigan dasturiy ta’minotga asoslangan shifrlashdan farqli o‘laroq, apparatli shifrlash qurilmalari shifrlash va shifrni ochish kalitlarini o‘zi tasodifiy ishlab chiqaradi, shuning uchun faqat vakolatli foydalanuvchilar maxfiy ma’lumotlarga kirishlari va undan foydalanishlari mumkin bo‘ladi.[3]

Apparat shifrlashning asosiy afzalligi shundaki, uni asosiy kompyuterning operatsion tizimiga o‘rnatish shart emas. Bu shuni anglatadiki, agar sizning operatsion tizimingiz buzilgan bo‘lsa ham, apparat shifrlash jarayonlari ma’lumotlaringizni xavfsiz saqlaydi. Shifrlash jarayonlari har doim yoqilgan, shuning uchun ular shifrlash protokollarini o‘chirish uchun dasturlashtirilgan zararli dasturlar yoki kiberhujumlarga bardoshlidir. Bundan tashqari, qo‘pol kuch hujumlari shifrlash qurilmalarida samarasiz, chunki ular bir necha muvaffaqiyatsiz autentifikatsiya urinishlaridan keyin foydalanuvchilarni blokirovka qiladi va urinishlar sonini dasturiy ta’minotga asoslangan shifrlashda bo‘lgani kabi qayta belgilashning imkoni yo‘q. Bundan tashqari, shifrlash qurilmalari va ularning jarayonlari asosiy kompyuterdan alohida

ishlayotganligi sababli, unumdorlik bilan bog‘liq muammolarga duch kelmaysiz. Apparat shifrlash shuningdek, asosiy kompyuterda murakkab konfiguratsiyalar yoki drayverlarni o‘rnatishni talab qilmaydi, bu uni juda intuitiv xavfsizlik yechimiga aylantiradi. [4]

Apparatga asoslangan shifrlash va dasturiy ta’minotga asoslangan shifrlash orasidagi farq.

№	Dasturiy ta’minotga asoslangan shifrlash	Apparatga asoslangan shifrlash
1	Apparatga qaraganda ancha arzon va tejamkor	Dasturiy ta’minotga qaraganda ancha qimmat va ko‘p resurs talab etadi
2	Dasturiy vositalar moslashuvchan ular istalgan kompyuter yoki qurulmalarga o‘rnatilishi mumkin	Apparatga asoslangan shifrlash maxsus qurilmalar hisoblanib ular asosan tor doiradagi qurilmalarga o‘rnatiladi
3	Apparatga qaraganda xavfsizlik darajasi ancha zaif hisoblanadi	Dasturiy ta’minotga qaraganda xavfsizlik masalasi ancha yuqori
4	Qurilma operatsion tizimiga uzviy bog‘liq ravishda bitta protsessorda ishlaydi,bu esa tizim ishlashini sekinlashtiradi	Qurilma operatsion tizimiga bog‘liq emas chunki u alohida ajratilgan shifrlangan disk protsesorida ishlaydi,bu esa tizim ishlashiga ta’sir qilmaydi
5	Qo‘pol kuch hujumiga bardoshsiz chunki buzg‘unchi tizimga kirib urunishlar sonini ko‘paytirishi mumkin	Qo‘pol kuch hujumiga bardoshli chunki tizim buzg‘unchini avtomatik bloklaydi
6	Windows Bitlocker va Mac FileVault dasturlarida ma’lumotlarni qayta tiklash mumkin agarda u oldindan yoqilgan bo‘lsa	Ma’lumotlarni qayta tiklashning deyarli imkoni yo‘q.Chunki apparat vositalar qurilma o‘g‘irlanganda ham xavfsizlikni ta’minlash uchun yaratilgan
7	Arzonligi sababli amaliyotda keng foydalaniladi	Qimmatligi sababli asosan katta tashkilotlar va davlat korxonalarida foydalaniladi
8	Yangilanishlarni avtomatik shifrlash dusturini yangi versiyasini o‘rnatish orqali amalga oshirish mumkin	Apparat shifrlash xotira qurilmasining o‘ziga o‘rnatilganligi sababli,qurilmaning o‘zini kuchliroq shifrlash qobiliyatiga ega bo‘lgan boshqasi bilan almashtirish kerak bo‘ladi.

Siz foydalanadigan shifrlash turi oxir-oqibat kompaniyangiz ehtiyojlariga bog‘liq bo‘ladi. Haqiqatan ham muhimi, ish unumdorligiga ta’sir qilish, xavfsizlik talablari va byudjet kabi omillarni hisobga olishdir. Xususan cheklangan byudjetga ega bo‘lgan korxonalar moslashuvchanligi va kengaytirilishi tufayli dasturiy ta’minotga asoslangan shifrlashdan foydalanishi maqsadga muvofiqdir.

Biroq, apparatga asoslangan shifrlashdan foydalanish katta korporatsiyalar, moliya, sog‘liqni saqlash va davlat sektoridagi tashkilotlar uchun eng maqbul yechimdir. Moliyaviy pul aylanmalari, sog‘liqni saqlash tizimi va davlat tashkilotlarida

xavfsizlik o‘ta nozik masala shu sababli kuchli shifrlangan qurilmalardan foydalangan holda ushbu ko‘rsatmalarga rioya qilish orqali siz xavfsizlikni kriptografik himoyasidan to‘laqonli himoya sifatida foydalanishingiz mumkin.

FOYDALANILGAN ADABIYOTLAR RO‘YXATI: (REFERENCES)

1. www.geeksforgeeks.org
2. www.dsolutionsgroup.com
3. www.ontrack.com
4. Z. Liu, E. Wenger, and J. Großschädl, MoTE-ECC: Energy-Scalable Elliptic Curve Cryptography for Wireless Sensor Networks, pp. 361–379. Cham: Springer International Publishing, 2014.
5. “Kriptografiyaning matematik asoslari” O‘quv qo‘llanma: D.Y.Akbarova, O.P.Axmedova, I.U.Xolimtoyeva, X.P.Xasanov, P.F.Xasanov