O‘Z-O‘ZINI SHIFRLOVCHI DISKLARDA APPARAT SHIFRLASHNI AMALGA OSHIRISH

D.T. Xurramov
(Katta o‘qituvchi, Muhammad al-Xorazmiy nomidagi TATU)

U.S. Ahmadov
(magistrant, Muhammad al-Xorazmiy nomidagi TATU)
E-mail: ahmadovulugbek98@gmail.com

ANNOTATSIYA

Raqamli ma’lumotlarning uchta holati mavjud bo‘lib, ularning har biri kiberhujumlarga juda zaifdir: uyqu rejimidagi ma’lumotlar, harakatdagi ma’lumotlar va foydalanilayotgan ma’lumotlar. Bularning har biri tegishli himoyaga muxtoj va ularning o‘ziga xos pozitsiyalari tufayli ushbu himoyani ta’minlash uchun oddiy antivirus dasturidan tortib, apparatga asoslangan to‘liq disk shifrlashgacha bo‘lgan turli xil usullarni talab qiladi. Bugun ushbu bayonotda ikkinchisiga ko‘proq urg’u berilgan , chunki bu bugungi kunda uyqu rejimida malumotlarni himoya qilish bo‘yicha eng samarali usullardan biri hisoblanadi.

O‘Z-O‘ZINI SHIFRLAYDIGAN DISKLAR

O‘z-o‘zini shifrlaydigan disklar (SED) - bu foydalanuvchi kiritishi yoki diskni shifrlash dasturiga ehtiyoj sezmasdan, diskdagi ma’lumotlarni avtomatik ravishda shifrlash va deshifrlash uchun mo‘ljallangan qattiq disk (HDD) yoki (SSD).SED shifrlash jarayoni shaffof chunki foydalanuvchi yoki tizim ilovalari dasturiy ta’minotiga mutlaqo bexabar bo‘lishi uchun mo‘ljallangan. Bu sezilmaydigan jarayon shaffof shifrlash deb nomlanadi. Ushbu jarayonning ma’lumotlar xavfsizligi uchun qanchalik foydali ekanligini keyingi bo‘limda muhokama qilamiz.

Aslida, SED ishlab chiqaruvchidan chiqib, xost tizimida yoqilgan paytdan boshlab, diskka yoziladigan va o‘qiladigan ma’lumotlar doimiy ravishda shifrlanadi va deshifrlanadi. Dasturiy ta’minotga asoslangan disk shifrlash yechimlaridan farqli o‘laroq, disk ma’lumotlarini shifrlash va shifrini ochish uchun qo‘shimcha qadamlar kerak emas. Uskunaga asoslangan to‘liq disk shifrlash bilan siz shunchaki tizimingizni yoqasiz va odatdagidek ishni davom ettirasz.

Samsung, Seagate va Toshiba kabi bir qancha yirik texnologiya va ma’lumotlarni saqlash kompaniyalari bugungi kunda bozorda o‘zlarining maxsus SED-lariga ega. Ularni mavjud server yoki ish stantsiyasiga o‘rnatish uchun uni sotib olish mumkin

yoki ishonchli tizim ishlab chiqaruvchisidan siz tanlagan yechimda oldindan o‘rnatilgan holda sotib olish mumkin.[5]

O‘Z-O‘ZINI SHIFRLOVCHI DISKLARDA APPARAT SHIFRLASH

O‘z-o‘zini shifrlovchi disklar bilan shifrlash har doim yoniq bo‘ladi, ya’ni ma’lumotlar SEDga yozilsa, u qurilma tomonidan shifrlanadi va keyin SED dan o‘qilganda deshifrlanadi. Parol xavfsizligi funksiyasi shifrlashni boshqarish dasturi tomonidan faollashtirilishi kerak. Agar bu bajarilmasa, foydalanuvchiga diskdagi ma’lumotlarni o‘qishga hech narsa to‘sqinlik qilmaydi. Boshqacha qilib aytadigan bo‘lsak, SED, agar buni oldini olish uchun xavfsizlikni boshqarish dasturi o‘rnatilmagan bo‘lsa, so‘ragan har bir kishi uchun barcha ma’lumotlarning shifrini hal qiladi.[1]

APPARAT SHIFRLASHNING AFZALLIKLARI

SED texnologiyasi tasdiqlangan va sertifikatlangan ma’lumotlar xavfsizligini ta’minlaydi, bu foydalanuvchi ma’lumotlari uchun yuklashdan oldin deyarli buzilmaydigan himoyani ta’minlaydi. Shifrlash disk boshqaruvchisining bir qismi bo‘lgani uchun u yuklashdan oldin ma’lumotlarni himoyasini to‘laligicha ta’minlaydi. Autentifikatsiya kodlarini tekshirish uchun dasturiy yordam dasturini ishga tushirish mumkin emas, chunki shifrlash har qanday dasturiy ta’minot yuklashni boshlashdan oldin faol bo‘ladi. Bundan tashqari, shifrlash va deshifrlash SED-da bo‘lganligi sababli shifrlash kalitlari kontrollerning o‘zida saqlanadi va hech qachon drayverni tark etmaydi.[4]

APPARAT SHIFRLASH VA DASTURIY SHIFRLASH

SSD disklarida dasturiy ta’minotni shifrlash o‘rniga apparat shifrlashdan foydalanishning asosiy afzalligi shundaki, apparat shifrlash xususiyati diskning qolgan qismi bilan optimallashtirilgan. Agar foydalanuvchi dasturiy ta’minotni shifrlashni xotira drayveriga qo‘llasa, bu diskka yozish jarayoniga bir necha qo‘shimcha qadamlar qo‘shadi, chunki ma’lumotlar yozilayotganda shifrlash dasturi tomonidan shifrlanishi kerak. O‘sha ma’lumotlar foydalanuvchi unga kirishni xohlasa, dasturiy ta’minot tomonidan yana shifrlanishi kerak, bu esa ishlash jarayonini sekinlashtiradi. Boshqacha qilib aytganda, dasturiy ta’minotni shifrlash qatlamini qo‘shish SSD ishlashiga salbiy ta’sir qiladi. Biroq, SED ning apparat shifrlashi kontrollerga birlashtirilgan, ya’ni qisqa muddatda ham, uzoq muddatda ham SSD ishlashiga hech qanday ta’sir ko‘rsatmaydi. O‘qish va yozish tezligi allaqachon shifrlashni hisobga olgan holda amalga oshiriladi, chunki u har bir yozish siklida sodir bo‘ladi va parol hal qilish har bir o‘qish siklida sodir bo‘ladi. Shifrlash diskning oddiy ishlashining bir qismidir.[3]

Apparatga asoslangan o‘z-o‘zini shifrlash disklari dasturiy ta’minotga asoslangan echimlardan ustundir.

Apparatga asoslangan o‘z-o‘zini shifrlovchi disklar	Dasturiy ta’minotga asoslangan shifrlangan disklar
Shaffoflik: Tizim yoki dasturga qo‘shimchalar kiritish shart emas.	Shaffof emas: Diskni shifrlash tizim qo‘shimcha dasturlarni talab qiladi.
Shifrlash kalitini generatsiya qilish yoki shifrlash va deshifrlash uchun foydalanuvchining ishtiroki shart emas,bu jarayon avtomatik tarzda amalga oshiriladi.	Kalit generatsiya qilish hamda ma’lumotlarni shifrlash va deshifrlash jarayoni foydalanuvchi tomonidan amalga oshiriladi
SED bortda saqlanib qolgan kalitlarni butkul o‘chirib yuboradi.	Kalit bortda saqlanib qoladi
Tizimga kirgan buzg’unchi SED dan to‘laqonli foydalana oladi.	Tizimga kirgan buzg’unchi shifrlash dasturiga kirolmasa shifrlangan ma’lumotlardan foydalana olmaydi.
SED lar tizim dasturlari ishlash tezligiga umuman ta’sir o‘tkazmaydi.	Shifrlash va boshqa dasturiy vositalar bitta protsessorda orqali amalga oshirilgani sababli tizim ishlash tezligiga sezilarli darajada ta’sir o‘tkazadi[2].

USKUNANI SHIFRLASHNI FAOLLASHTIRISH

Foydalanuvchiga SED ning shifrlash qobiliyatidan foydalanishi kerak bo‘lgan yagona narsa SED qurilmalari uchun shifrlash kalitlarini boshqarishni ta’minlovchi dasturiy yordam dasturidir. Muhim SEDlar MicrosofteDrive standartiga to‘liq mos keladi, bu WindowsBitLocker yordamida oddiy plaginni o‘rnatish orqali ma’lumotlar xavfsizligini ta’minlaydi. Windows BitLocker diskni ishlatishdan oldin uni shifrlashi shart emasligi sababli (bu SSD boshqaruvchisi tomonidan amalga oshirilgan) hech qanday kechikish kuzatilmaydi. Siz qilishingiz kerak bo‘lgan yagona narsa, o‘z-o‘zini shifrlash diskiga avvalgidek ishlashiga ruxsat berish va apparatga asoslangan shifrlash diskining himoyasi va yuqori unumdorligidan bahramand bo‘lishdir.

Umuman olganda ma’lumotlarni kriptografik himoyalashda dasturiy ta’minotga qaraganda apparatga asoslangan shifrlash vositalari himoyani samaraliroq ta’minlaydi.SED texnalogiyasi alohida diskni shifrlash dasturlariga qaraganda ancha xavfsiz va foydalanuvchidan yuqori bilim darajasini talab qilmaydi. Ushbu apparat vositadan foydalanish malumotlar xavfsizligini yetarli darajada ta’minlabgina qolmay foydalanuvchiga ko‘plab qulayliklarni yaratadi.

FOYDALANILGAN ADABIYOTLAR RO‘YXATI: (REFERENCES)

1. https://trentonsystems.com
2. https://trustedcomputinggroup.org
3. https://crucial.com
4. “Kriptografiyaning matematik asoslari” O‘quv qo‘llanma: D.Y.Akbarova, O.P.Axmedova, I.U.Xolimtoyeva,X.P.Xasanov,P.F.Xasanov
5. https://ibm.com