TARMOQLARDA AUTENTIFIKASIYA PROTOKOLLARIGA QO'LLANILADIGAN NAMUNAVIY HUJUM TURLARI

[1]Rustamov Alisher Bahodirovich
Muhammad al-Xorazmiy nomidagi TATU Qarshi filiali o'qituvchisi
arustamov_88@mail.ru,
[2]Amirov Akbarshox Dilshod o'g'li
Muhammad al-Xorazmiy nomidagi TATU Qarshi filiali talabasi
amirovakbarshoh05@gmail.com Tel:+998912150812.
https://doi.org/10.5281/zenodo.7493523

Axborot komunikasiya tizimlarida orqali uzatiladigan axborot jamiyat rivojining muhim shartlaridan biri bo'lib qoldi. U ishlab chiqarish resursi, insonlar orasidagi aloqani ta'minlovchi qudratli vositaga aylandi. Shu bois davlat hokimiyati va boshqaruvi organlari, umuman, jamiyatning axborot uzatish tezligi hamda sifatiga bo'lgan talablari kun sayin ortib bormoqda. Ma'lumki, absolyut xavfsiz tizimlar mavjud emas, lekin «ishonish mumkin bo'lgan tizim» ma'nosidagi ishonchli tizimlardan foydalaniladi. Yetarlicha apparat va dasturiy vositalardan foydalanib, bir vaqtning o'zida turli maxfiylik darajasidagi ma'lumotlarni foydalanuvchilar guruhi tomonidan foydalanish huquqlarini buzmagan holda qayta ishlash imkonini beruvchi tizim ishonchli hisoblanadi.

Axborot kommunikatsiya tizimlarida axborot xavfsizligi muammosini yechish uchun kriptografik usullar ichida eng muhimlaridan biri autentifikatsiya masalasidir. Autentifikasiya deganda ishtirokchining dastur, qurilma yoki ma'lumotlarning haqiqiyligini belgilash tartiboti tushuniladi. Autentifikasiya ishtirokchi haqiqatan aynan o'zi ekanligiga ishonch hosil qilishga imkon beradi

Autentifikasiya protokollariga qo'llaniladigan namunaviy hujum turlari asosan sakkiz turda bo'lib ular quyidagilardan iborat:

1. *Xabarni qayta yuborish hujumi* - bu hujumda buzg'unchi avvaldan protokolning oldingi seansida tutib olingan eski xabarni yozib qo'yadi va uni yangi seansda qayta yuboradi.
2. *"O'rtadagi odam" hujumi* - bu hujum asosan o'zaro autentifikasiya qilishni ko'zda tutmaydigan protokollarga qo'llaniladi. Bunday hujum asnosida buzg'unchi protokol ishtirokchilaridan birining qiyin savollarini boshqa ishtirokchiga jo'natishi va unga javob olishi keyin so'rovchiga yuborishi mumkin va aksincha.
3. *Parallel seans yordamidagi hujum* - bu hujumda buzg'unchi boshchiligida bir nechta protokol bajariladi. Parallel seanslar buzg'unchiga biror seansdagi qiyin savollarga javob uchun boshqa seanslarda olingan axborotdan foydalanish imkonini beradi.

4. *Xabarlarni akslantirish yordamida hujum* - xabarlarni akslantirish yordamida hujumda buzg'unchi qonuniy ishtirokchini keyingi kriptografik ishlov berish uchun o'zining sherigiga yuborgan xabarni tutib qoladi va uni orqaga qaytarib yuboradi. Bunda akslantirilgan xabar "orqaga qaytarilgan xabarning" aynan o'zi bo'lmaydi, chunki buzg'unchi quyi darajali protokol bilan ismi va manzilini o'zgartiradi, shuning uchun xabarning muallifi o'z matnini tanimaydi.

5. *Xabar almashinuvi yordamida hujum* – bu hujum vaqtida buzg'unchi bir nechta protokollarning xabarlarni almashtirib amalga oshiradi. Buzg'unchi xabar tuzadi va uni protokol ishtirokchilaridan biriga yuboradi va javobini kutadi. So'ngra u olingan javobni ikkinchi ishtirokchiga boshqa protokol doirasida yuboradi, uning javobini olgandan so'ng keyingi ishtirokchiga jo'natadi va hokazo.

6. *Noto'g'ri talqin etish asosidagi hujum* – bu hujumda buzg'unchi qonuniy ishtirokchining xabarni yoki xabarlar to'plamini ma'nosini aniqlay olmaganidan foydalanadi. Ko'pincha noto'g'ri talqin etish ishtirokchiga tasodifiy sonni, vaqt belgisi (VB)ni, ism, shifrlangan kalitni aldash yo'li bilan noto'g'ri talqin etishiga majburlaganda paydo bo'ladi.

7. *Nomsiz xabarlar asosidagi hujum* - Autentifikasiyalash protokollarida xabar muallifi ismini va shifrlash kalitini kontekstdan aniqlash mumkin. Ammo ba'zan bunday qilish mumkin bo'lmasligi, ya'ni ismining yo'kligi katta muammolarni keltirib chiqaradi.

8. *Kriptografik amallarni noto'g'ri bajarishga asoslangan hujum* – bu hujum protokollardagi eng keng tarqalgan nuqson hisoblanib, bu kamchilak ikki holatda paydo bo'ladi:

1) Ma'lumotlar yaxlitligi himoyasining mavjud emasligi oqibatidagi hujum. Bunda buzg'unchi ma'lumotlar yaxlitligi himoyasining mavjud emasligi oqibatida zaiflashgan protokolga hujum qiladi.

2) "Ma'noga ega turg'unlik" mavjud emasligi oqibatidagi maxfiylikning buzilishi. Protokol nuqsonidan foydalangan buzg'unchi shifrlangan matndagi maxfiy xabar haqidagi qisman ma'lumotni olishi mumkin va kriptoprotokolni buzmagan holatda "hammasi yoki hyech narsa" prinsipidagi hujumni tashkil etishi mumkin.

Xulosa qilib aytganda axborotni himoya qilishda hozirda autentifikasiya protokollari keng qo'llanilib kelinayotganligini tushinishimiz mumkin. Autentifikasiya protokollariga qo'llaniladigan namunaviy hujumlarning g asosan sakkiz turlarini ko'rib o'tdik. Tarmoqlarda ma'lumotlar almashinish jarayonida nimalarga e'tibor berishimiz va ma'lumotlarni kuchli himoya qilishimiz uchun kompleks chora-tadbirlar ishlab chiqish va amalda qo'llash muhimdir.

Foydalanilgan adabiyotlar:

1. O'zbekiston Respublikasi Prezidentining «O'zbekiston Respublikasi Milliy axborot-kommunikasiya tizimini yanada rivojlantirish chora tadbirlari to'g'risida»gi № PQ-1989 qarori, 27 iyun 2013 yil.
2. O`z DST 1092:2009 "Axborot texnologiyasi. Axborotning kriptografik muhofazasi. Elektron raqamli imzoni shakllantirish va tekshirish jarayonlari".
3. O`z DST 1105:2009 "Axborot texnologiyasi. Axborotning kriptografik muhofazasi. Ma'lumotlarni shifrlash algoritmi".
4. O'z DSt 1092:2009. Axborot texnologiyasi. axborotning kriptografik muhofazasi. Elektron raqamli imzoni shakllantirish va tekshirish jarayonlari.
5. ГОСТ Р 34.11-94. Криптографическая защита информации. Функция хэширования.