MULTIMEDIALI TARMOQLARDA QO‘LLANILADIGAN XAVFSIZLIK PROTOKOLLARI

Suyunov Muzaffarjon Nurmurot o‘g‘li
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti
muzaffarsuyunov1997@gmail.com
https://doi.org/10.5281/zenodo.16352007

ARTICLE INFO

Qabul qilindi: 07-Iyul 2025 yil
Ma’qullandi: 11-Iyul 2025 yil
Nashr qilindi: 23-Iyul 2025 yil

KEY WORDS

Multimediali tarmoqlar, Tarmoq xavfsizligi, Xavfsizlik protokollari, OSI modeli, IPsec, SSL/TLS,HTTPS, Kerberos, SNMPv3, DTLS, SFTP, RTP/RTSP, Shifrlash,Autentifikatsiya, Kiberxavfsizlik, Ma’lumotlar yaxlitligi, Tarmoqlarni himoyalash, VPN xavfsizligi, Tarmoq sathlari, Real vaqt rejimi..

ABSTRACT

Ushbu maqolada multimediali tarmoqlarda qo‘llaniladigan asosiy xavfsizlik protokollari va ularning funksional xususiyatlari yoritilgan. Dastlab tarmoq xavfsizligi va OSI modeli qatlamlari haqida umumiy ma’lumot berilib, har bir xavfsizlik protokoli qaysi qatlamda ishlashi va qanday tahdidlarga qarshi xizmat qilishi izohlangan. Protokollar qatorida IPsec, SSL/TLS, DTLS, Kerberos, SNMP, HTTP/HTTPS kabilar tahlil qilinadi. Har bir protokolning afzalliklari, kamchiliklari va qo‘llanish sohasi alohida ko‘rib chiqilgan. Shuningdek, maqola oxirida protokollar taqqoslanib, ular multimedia tarmoqlarining xavfsizligi uchun qanchalik muhim ekani ta’kidlangan. Mazkur maqola tarmoq xavfsizligi bilan shug‘ullanuvchi mutaxassislar, talabalar va axborot xavfsizligi sohasi tadqiqotchilari uchun foydali manba bo‘la oladi

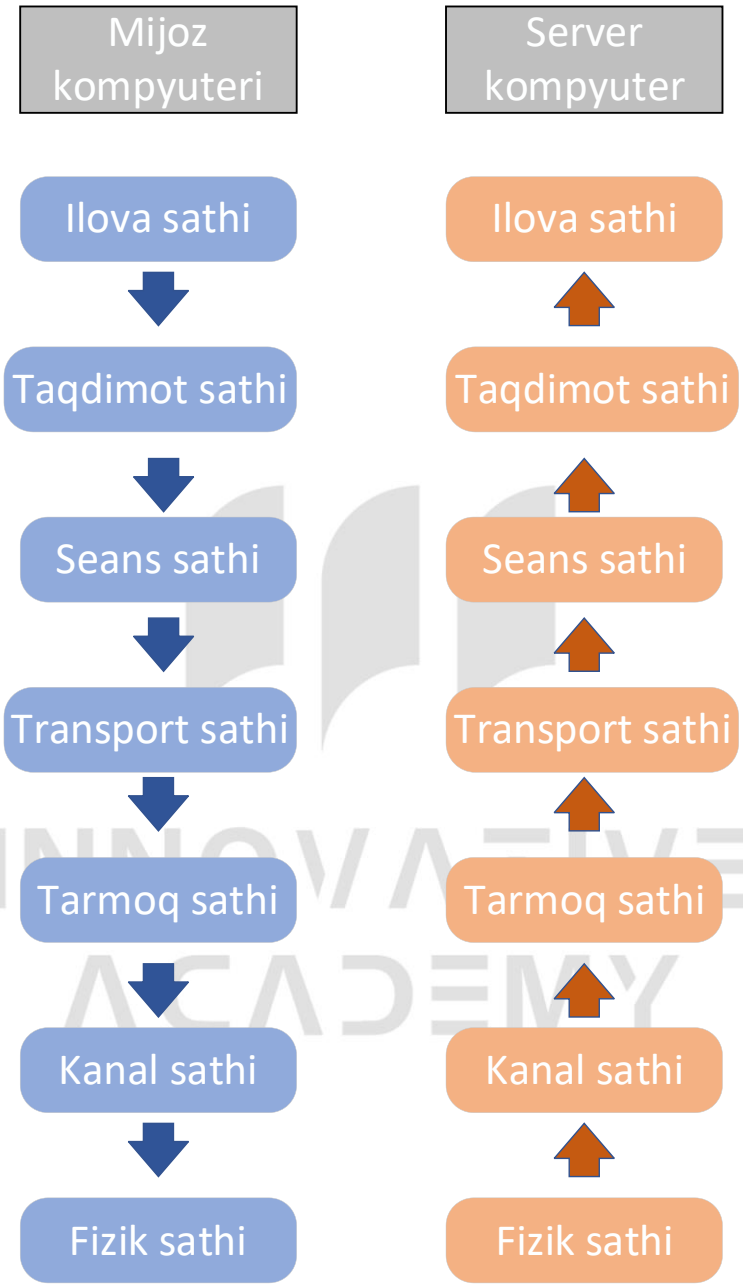
Tarmoq xavfsizligi, kiberxavfsizlikning ixtisoslashgan sohasi, tashkilotlar o‘z tarmoqlari va har qanday tarmoq aktivlari yoki trafigini himoya qilish uchun foydalanadigan siyosatlar, protseduralar va texnologiyalarni o‘z ichiga oladi. Sanoat yoki hajmdan qat'iy nazar, barcha tashkilotlar ma'lumotlar yo‘qolishi, ruxsatsiz kirish va tarmoqqa asoslangan hujumlar kabi tahdidlarga qarshi tayyorlanishi kerak.

Tarmoq xavfsizligi protokollari tarmoq ulanishlari orqali uzatiladigan ma'lumotlarning yaxlitligi va xavfsizligini ta'minlaydigan tarmoq protokollaridir. Amaldagi maxsus tarmoq xavfsizligi protokoli himoyalangan ma'lumotlar turiga va tarmoq ulanishiga bog'liq. Har bir protokol tarmoq ma'lumotlarini ruxsatsiz yoki zararli ma'lumotlarni o‘qish yoki olib tashlashga urinishlardan himoya qilish uchun zarur bo‘lgan texnika va protseduralarni belgilaydi.

Open Systems Interconnection (OSI) ilovalarning tarmoqlar orqali qanday bog'lanishini ko‘rsatadigan mos yozuvlar modelidir. U jismoniy simlardan tortib, tarmoq orqali boshqa qurilmalar bilan bog'lanishga harakat qiladigan ilovalargacha bo‘lgan har bir aloqa qatlami qanday qilib bir-birining ustiga qurilganligini ko‘rsatadi (1-rasm).

OSI - bu tarmoq yoki aloqa tizimining imkoniyatlarini tavsiflovchi aniq asosni ta'minlovchi, o‘zaro ishlaydigan dasturiy ta'minot va apparat vositalarini loyihalash bo‘yicha

texnologiya sotuvchilarni yo‘naltiruvchi mos yozuvlar modeli. Xavfsizlik guruhlari uchun OSI modeli tarmoqning qaysi qatlamlarini himoya qilish kerakligini, muayyan xavfsizlik tahdidlari qayerda paydo bo‘lishi mumkinligini va ularni qanday oldini olish va yumshatish kerakligini tushunishga yordam beradi.



2.1-rasm. **OSI modeli sathlari.**

OSI modeli quyidagi qatlamlarni o‘z ichiga oladi:

1-sath – fizik sathi - tarmoq tugunlari orasidagi fizik kabel yoki simsiz ulanish.

2-sath — kanal sathi — ulanishlarni yaratadi va tugatadi, paketlarni freymlarga ajratadi va ularni manbadan manzilga uzatadi.

3-sath — tarmoq sathi — segmentlarni tarmoq paketlariga ajratadi va qabul qilingandan so‘ng ularni qayta yig‘adi va jismoniy tarmoqdagi optimal yo‘l yordamida paketlarni yo‘naltiradi.

4-sath — transport sathi — qabul qiluvchi tomondagi segmentlarni qayta yig‘ish, uni

seans qatlami tomonidan ishlatilishi mumkin bo‘lgan ma’lumotlarga aylantirish uchun javobgardir.

5-sath - seans sathi - qurilmalar o‘rtasida seanslar deb ataladigan aloqa kanallarini yaratadi. Seanslarni ma'lumotlarni uzatish vaqtida ochiq tutadi va tugashi bilan ularni yopadi.

6-sath — taqdimot sathi — amaliy qatlam uchun ma’lumotlarni tayyorlaydi, bunda ikkita qurilma to‘g‘ri qabul qilinishini ta’minlash uchun ma’lumotlarni kodlash, shifrlash va siqish usullarini belgilaydi.

7-sath - ilova sathi - veb-brauzerlar va elektron pochta mijozlari kabi oxirgi foydalanuvchi dasturlari tomonidan qo‘llaniladi. HTTP, FTP va DNS kabi protokollardan foydalangan holda oxirgi foydalanuvchilar uchun muhim bo‘lgan ma'lumotlarni yuboradi va oladi.

Quyida eng keng tarqalgan tarmoq xavfsizligi protokollari keltirilgan. Ular pastdan yuqoriga qarab ishlaydigan tarmoq sathi tomonidan tartibga solinadi.

Internet Protocol Security (IPsec) Protokoli — OSI 3-sath

IPsec - bu Internet kabi umumiy tarmoqlar orqali uzatiladigan ma'lumotlarni himoya qiluvchi protokol va algoritmlar to‘plami. 1990-yillarda Internet Engineering Task Force (IETF) IPsec protokollarini chiqardi. Ular IP-qatlam xavfsizligini ta'minlash uchun tarmoq paketlarini shifrlaydi va autentifikatsiya qiladi.

IPsec dastlab ESP va AH protokollarini o‘z ichiga olgan. Encapsulating Security Payload (ESP) ma'lumotlarni shifrlaydi va autentifikatsiyani ta'minlaydi, Autentifikatsiya sarlavhasi (AH) esa takroriy o‘ynashga qarshi imkoniyatlarni taklif qiladi va ma'lumotlar yaxlitligini himoya qiladi. O‘shandan beri to‘plam xavfsizlik
assotsiatsiyalarini (SA) o‘rnatish uchun umumiy kalitlarni taqdim etuvchi Internet Key Exchange (IKE) protokolini o‘z ichiga olgan holda kengaytirildi. Bular xavfsizlik devori yoki router orqali shifrlash va shifrni ochish imkonini beradi.

IPsec maxfiy ma'lumotlar va VPN-larni himoya qila oladi, ma'lumotlar uzatishni shifrlash uchun tunnellashni ta'minlaydi. U dastur sathida ma'lumotlarni shifrlashi va shifrlashsiz autentifikatsiyani yoqishi mumkin.

SSL va TLS - OSI 5-sathi

Secure Sockets Layer (SSL) protokoli ma'lumotlarni shifrlaydi, ma'lumotlarning kelib chiqishini autentifikatsiya qiladi va xabarning yaxlitligini ta'minlaydi. Mijoz va server autentifikatsiyasi uchun X.509 sertifikatlaridan foydalanadi. SSL serverni qo‘l siqish orqali autentifikatsiya qiladi, xavfsizlik seansi parametrlarini muhokama qiladi va seans kalitlarini yaratadi. Keyin u kelib chiqishini tasdiqlash orqali ma'lumotlarni xavfsiz tarzda uzatishi mumkin.

SSL seanslari mijoz va server tomonidan ishlatiladigan algoritmlarga o‘xshash kriptografik algoritmlardan foydalanadi (qo‘l siqish paytida aniqlanadi). Serverlar AES va Triple DES kabi algoritmlar bilan shifrlashni qo‘llab-quvvatlashi mumkin.

X.509 server sertifikatlari SSL uchun talab bo‘lib, mijozga serverni tekshirish imkonini beradi. SSL autentifikatsiya qilish uchun X.509 mijoz sertifikatlaridan ham foydalanishi mumkin. Ushbu sertifikatlar server kalitlaridagi ishonchli sertifikat organi tomonidan imzolanishi kerak.

Transport Layer Security (TLS) bu IETF tomonidan belgilangan SSL-ga asoslangan protokol (SSL emas).

Datagram Transport Layer Security (DTLS) — OSI 5-sathi

DTLS - bu TLS-ga asoslangan datagram aloqasi xavfsizligi protokoli. Bu xabarlarni yetkazib berish yoki xabarlar tartibda kelishini kafolatlamaydi. DTLS datagram protokollarining afzalliklarini taqdim etadi, jumladan, past kechikish va qisqartirilgan qo‘shimcha xarajatlar.

Kerberos protokoli - OSI 7-sathi

Kerberos - umumiy Internet kabi ishonchsiz tarmoqlar uchun xizmat so‘rovini autentifikatsiya qilish protokoli. U ishonchli xostlar o‘rtasidagi so‘rovlarni autentifikatsiya qiladi va o‘rnatilgan Windows, Mac va Linux operatsion tizimini
qo‘llab-quvvatlaydi.

Windows Kerberos-dan standart autentifikatsiya protokoli va Active Directory (AD) kabi xizmatlarning asosiy komponenti sifatida foydalanadi. Keng polosali xizmat ko‘rsatuvchi provayderlar undan o‘z tarmoqlariga kiruvchi pristavkalar va kabel modemlarini autentifikatsiya qilish uchun foydalanadilar.

Tizimlar, xizmatlar va foydalanuvchilar Kerberosdan foydalanganda faqat KDC ga ishonishlari kerak. KDC autentifikatsiyani taklif qiladi va tugunlarga bir-birini autentifikatsiya qilish uchun chiptalar beradi. Kerberos paketlarni autentifikatsiya qilish va uzatish vaqtida ularni himoya qilish uchun umumiy maxfiy kriptografiyadan foydalanadi.

Simple Network Management Protocol (SNMP) - OSI 7-sathi

SNMP - bu dastur sathida ishlaydigan tarmoq qurilmalarini boshqarish va monitoring protokoli. U LAN yoki WAN tarmog'idagi qurilmalarni himoya qilishi mumkin. SNMP serverlar va marshrutizatorlar kabi qurilmalarga tarmoqni boshqarish tizimi orqali muloqot qilish imkonini beradigan umumiy tilni taqdim etadi. SNMP IETF tomonidan belgilangan Internet protokollar to‘plamining asl qismidir.

SNMP arxitekturasining tarkibiy qismlariga menejer, agent va boshqaruv axborot bazasi (MIB) kiradi. Menejer - mijoz, agent - server va MIB - ma'lumotlar bazasi. SNMP agenti menejerning so‘rovlariga MIB yordamida javob beradi. SNMP keng tarqalgan bo‘lsa-da, ma'murlar protokolni amalga oshirish uchun agentlar va tarmoq boshqaruvi tizimi o‘rtasidagi aloqani yoqish uchun standart sozlamalarni o‘zgartirishlari kerak.

2004 yilda SNMPv3 ning joriy etilishi bilan SNMP protokoli uchta muhim xavfsizlik xususiyatiga ega bo‘ldi: tinglashning oldini olish uchun paketlarni shifrlash, paketlar tranzitda buzilmaganligiga ishonch hosil qilish uchun yaxlitlikni tekshirish va aloqa ma'lum manbadan kelganligini tekshirish uchun autentifikatsiya.

HTTP va HTTPS - OSI 7-sathi

HTTP - bu veb-fayllarni uzatish qoidalarini belgilaydigan dastur protokoli. Foydalanuvchilar veb-brauzerini ochganda bilvosita HTTP-dan foydalanadilar. U Internet protokollar to‘plamining tepasida ishlaydi.

HTTPS HTTP ning xavfsiz versiyasi bo‘lib, brauzerlar va veb-saytlar o‘rtasidagi aloqani ta'minlaydi. Bu maxfiy ma'lumotlarni uzatuvchi yoki qabul qiluvchi veb-saytlar uchun
muhim bo‘lgan DNS spoofing va o‘rtadagi odam hujumlarining oldini olishga yordam beradi. Foydalanuvchi loginlarini talab qiladigan yoki moliyaviy tranzaksiyalarni amalga oshiradigan barcha veb-saytlar jozibador ma’lumotlarni o‘g‘irlash maqsadlari bo‘lib, HTTPS dan foydalanishi kerak.

HTTPS umumiy ma'lumotlarni shifrlashni yoqish uchun ochiq kalitlardan foydalangan holda SSL yoki TLS protokoli orqali ishlaydi. HTTP sukut bo‘yicha 80-portdan foydalanadi, HTTPS esa xavfsiz uzatish uchun 443-portdan foydalanadi. HTTPS bilan server va brauzer ma'lumotlarni uzatishni boshlashdan oldin aloqa parametrlarini o‘rnatishi kerak.

Yuqorida keltirilgan protokollar multimedia tarmoqlarining xavfsizligi uchun juda muhimdir. Har bir protokol ma'lum bir maqsadda qo‘llaniladi va ma'lumotlar xavfsizligi nuqtai nazaridan turli xil xususiyatlarga ega (2.2-jadval).

2.2-jadval

Protokol	Maqsad	Foydalanish maydoni
SSL/TLS	Xavfsiz veb-aloqa kanalini ta'minlash	Veb-saytlar
SSH	Xavfsiz masofaviy kirishni ta'minlash	Serverni masofadan boshqarish
IPsec	IP-ga asoslangan tarmoqlarda ma'lumotlar xavfsizligini ta'minlash	Tarmoq trafigining xavfsizligi
SFTP	Fayl uzatish operatsiyalarida xavfsizlik	Fayl uzatish
RTP/RTSP	Real vaqt rejimida media oqimlari	Video va audio oqimlari
SNMPv3	Tarmoq boshqaruvini ta'minlash	Tarmoq boshqaruvi

Har bir protokol o‘zining afzalliklari va kamchiliklariga ega. Ba'zi protokollar xavfsizlikni oshiradi, boshqalari esa tezroq ma'lumotlarni uzatishni ta'minlaydi.

- SSL/TLS: U veb-saytlar o‘rtasida ma'lumotlarni uzatishda xavfsizlikni ta'minlash uchun ishlatiladi. SSL/TLS xavfsiz ulanishni o‘rnatish uchun server va mijoz o‘rtasida qo‘l siqish protokolidan foydalanadi. Afzalligi shundaki, u oxirigacha shifrlashni ta'minlaydi. Salbiy tomoni shundaki, ulanishni yaratish jarayoni uchun qo‘shimcha vaqt talab etiladi.
- SSH: Masofaviy kirish uchun ishlatiladigan protokol va tarmoq orqali ma'lumotlarni uzatish xavfsizligini ta'minlash uchun shifrlashdan foydalanadi. Afzalligi shundaki, u xavfsiz kirishni ta'minlaydi. Salbiy tomoni shundaki, u ba'zan ulanish uchun yuqori resurslardan foydalanishni talab qiladi.
- IPsec: Bu IP-ga asoslangan tarmoqlarda ma'lumotlar xavfsizligini ta'minlash uchun ishlatiladigan protokol. Afzalligi shundaki, u tarmoq trafigini shifrlashni ta'minlaydi. Kamchilik - o‘rnatishning murakkabligi.
- SFTP: Bu fayl uzatish operatsiyalarida xavfsizlik uchun ishlatiladigan protokol. Uning afzalligi shundaki, u shifrlash va autentifikatsiya kabi xavfsizlik choralarini ta'minlaydi. Salbiy tomoni - fayllarni uzatish operatsiyalarining sekinligi.
- RTP/RTSP: real vaqtda media oqimlari uchun foydalaniladigan protokol. Uning afzalligi shundaki, u yuqori tezlikda ma'lumotlarni uzatishni ta'minlaydi. Salbiy tomoni shundaki, xavfsizlik choralari cheklangan.

SNMPv3: Tarmoqni boshqarish protokoli va tarmoq trafigini himoyalash uchun shifrlashdan foydalanadi. Afzalligi shundaki, u tarmoq boshqaruvini soddalashtiradi. Salbiy tomoni

shundaki, u ba'zi hollarda yuqori protsessordan foydalanishni talab qiladi.

Foydalanilgan adabiyotlar:

1.R.I.Isayev, R.Atametov, R.Radjapovalarning “Telekommunikatsiya uzatish tizimlari”, Toshkent axborot texnologiyalari universiteti, Toshkent, 2011.
2.R.I.Isayev, D.X.Ibatova. “Multimediyali aloqa tarmoqlari”. Toshkent axborot texnologiyalari universiteti, Toshkent, 2019.
3. ITU-T Recommendation H.235 Version 2: Security and encryption for H-Series (H.323 and other H.245-based) mulitmedia terminals (2000).