IMS TIZIM OSTI SATHLARI STANDART PROTOKOLLARINI ISHLASHINI TAHLIL QILISH

Almardanov Muxriddin Xurram o‘g‘li
Muhammad al-Xorazmiy nomidagi TATU
Telekommunikatsiya injiniringi assistant

Annotatsiya: Internet orqali axborot uzatish jarayonida xavfsizlik masalalari dolzarb ahamiyat kasb etadi. Maxfiylik, ma’lumotlarning yaxlitligi va autentifikatsiyasi tarmoqlar uchun muhim talabdir. IPsec protokoli ushbu xavfsizlik talablarini qondirish uchun ishlab chiqilgan va hozirgi kunda VPN (Virtual Private Network) va korporativ tarmoqlarda keng qo‘llanilmoqda. Ushbu maqolada IPsec protokolining ish prinsipi va uning tarmoq xavfsizligidagi o‘rni ilmiy asosda tahlil qilinadi.

Kalit so‘zlar: *IMS, IP-sec prorotokoli, tarmoq xavfsizligi, AH, SPD, SAD.*

Abstract: Security issues are of great importance in the process of information transmission over the Internet. Confidentiality, data integrity and authentication are important requirements for networks. The IPsec protocol was developed to meet these security requirements and is currently widely used in VPN (Virtual Private Network) and corporate networks. This article analyzes the working principle of the IPsec protocol and its role in network security on a scientific basis.

Keywords: *IMS, IP-sec protocol, network security, AH, SPD, SAD.*

Kirish

IPsec (Internet Protocol Security) — internet protokoli (IP) orqali ma’lumotlarni xavfsiz uzatish uchun mo‘ljallangan xavfsizlik to‘plamidir. U tarmoqlar o‘rtasida ma’lumotlarni shifrlash, autentifikatsiya qilish va yaxlitligini ta’minlash vazifalarini bajarishda muhim rol kasb etadi.

IPSec protokollarining asosiy maqsadi IP tarmoqlari orqali ma’lumotlarni xavfsiz uzatishni ta’minlashdir. IPSec-dan foydalanish quyidagilarni kafolatlaydi:

-uzatiladigan ma’lumotlarning yaxlitligi, ya’ni uzatish paytida ma’lumotlar buzilmaydi, yo‘qolmaydi yoki takrorlanmaydi;

-jo‘natuvchining haqiqiyligi, ya’ni ma’lumotlar u o‘zini da’vo qilgan odam ekanligini isbotlagan jo‘natuvchi tomonidan uzatilgan;

-uzatiladigan ma’lumotlarning maxfiyligi, ya’ni ma’lumotlar ruxsatsiz ko‘rishga to‘sqinlik qiladigan shaklda uzatiladi.

Asosiy qism

IPes protokoli ochiq tarmoqning asosiy turi bo‘lgan IP tarmog‘i uchun OCI modelining tarmoq darajasida axborot almashinuvini himoya qilishning standart usullarini belgilaydi. Ushbu protokol IP protokolining (IPv6) yangi versiyasining bir qismidir va uning joriy versiyasiga (IPv4) ham amal qiladi. IPv4 protokoli uchun IPses-larni qo‘llab-quvvatlash maqsadga muvofiq va IPv6 uchun bu majburiydir.

IPSec - bu aniq yadroga ega bo‘lgan va yangi protokollar, algoritmlar va xususiyatlar bilan kengaytirilishi mumkin bo‘lgan ochiq standartlar tizimi. Standartlashtirilgan IP-larni himoya qilish funktsiyalari nazorat protokollari, konfiguratsiya protokollari va marshrutizatsiya protokollari kabi yuqori darajadagi protokollar tomonidan ishlatilishi mumkin.

Xavfsiz kanalni yaratish va ta’minlashning asosiy vazifalari quyidagilardan iborat :

xavfsiz kanal ishga tushirilganda foydalanuvchilar yoki kompyuterlarning identifikatsiyasini tekshirish;

xavfsiz kanalning uchinchi nuqtalari o‘rtasida uzatilgan ma’lumotlarni shifrlash va autentifikatsiya qilish;

Autentifikatsiya va ma’lumotlarni shifrlash protokollarini ishlatish uchun zarur bo‘lgan maxfiy kalitlar bilan kanal uchinchi nuqtalarini taqdim etish.

Yuqorida ko‘rsatilgan vazifalarni yechish uchun IPSes tizimi axborot almashish uchun xavfsizlik vositalari majmuini qo‘llaydi.

IPSec dasturlarining aksariyati quyidagi komponentlarga ega:. Asosiy protokol IPSec. Ushbu komponent ESP kapsülleme himoya protokoli va AH autentifikatsiya sarlavhasi protokolini amalga oshiradi. U sarlavhalarni qayta ishlaydi, paketga qo‘llaniladigan xavfsizlik siyosatini aniqlash uchun SPD va SAD ma’lumotlar bazalari bilan o‘zaro aloqada bo‘ladi;

IKE (Internet Key Exchange) kalit ma’lumot almashinuvini boshqarish protokoli. IKE odatda operatsion tizimga o‘rnatilgan dasturlar bundan mustasno, foydalanuvchi darajasidagi jarayon deb hisoblanadi;

Xavfsizlik siyosati bazasi (SPD). Bu eng muhim tarkibiy qismlardan biridir, chunki u paketga qo‘llaniladigan xavfsizlik siyosatini belgilaydi. SPD kiruvchi va chiquvchi paketlarni qayta ishlashda asosiy IPSec protokoli orqali qo‘llaniladi;

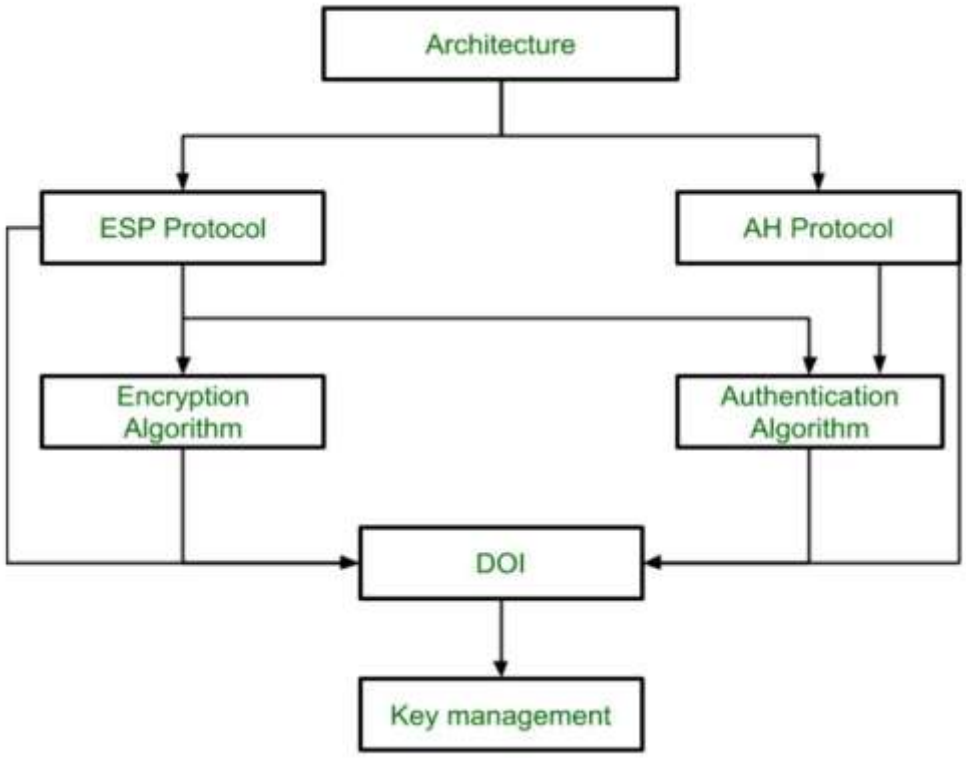
Xavfsizlik Assotsiatsiyasi bazasi (SAD). SAD ma’lumotlar bazasida kiruvchi va chiquvchi ma’lumotlarni qayta ishlash uchun xavfsiz SA (Xavfsizlik Assotsiatsiyasi) assotsiatsiyalari ro‘yxati saqlanmoqda. Chiqish SA’lari chiquvchi paketlarni himoya qilish uchun ishlatiladi va kiruvchi SA’lar IPSec sarlavhalari bilan paketlarni qayta ishlash uchun ishlatiladi. SAD ma’lumotlar bazasi SA tomonidan qo‘lda yoki IKE kalitlarini boshqarish protokoli yordamida to‘ldiriladi;

SA xavfsizlik siyosati va xavfsiz uyushmalarni boshqarish. Bu xavfsizlik siyosati va SA boshqaradigan dasturlar.

IPSec yadro protokoli (ESP va AHni amalga oshiradi) TCP / IP protokollari to‘plamining transport va tarmoq qatlamlari bilan chambarchas o‘zaro ta’sir qiladi. Aslida, IPSec protokoli tarmoq sathining bir qismidir. Asosiy IPSec protokol moduli ikkita interfeysni ta’minlaydi: kirish va chiqish. Kirish interfeysi kiruvchi paketlar tomonidan ishlatiladi va chiqish interfeysi chiquvchi paketlar tomonidan ishlatiladi. IPSec-ni amalga oshirish TCP / IP protokollari stekining transport va tarmoq qatlamlari o‘rtasidagi interfeysga bog‘liq bo‘lmasligi kerak.

SPD va SAD ma’lumotlar bazalari IPSec samaradorligiga sezilarli ta’sir ko‘rsatadi. SPD va SAD saqlash uchun ma’lumotlar tuzilishini tanlash IPSec ishlashiga bog‘liq bo‘lgan muhim nuqtadir. SPD va SADni amalga oshirish masalalari tizimning ishlashi va muvofiqligi talablariga bog‘liq.

IPSec tarkibiga kiritilgan barcha protokollarni ikki guruhga bo‘lish mumkin:
-uzatilgan ma’lumotlarni bevosita qayta ishlaydigan protokollar (ularning himoyasini ta’minlash uchun);
-Protokollarning birinchi guruhi uchun zarur bo‘lgan xavfsiz ulanish parametrlarini avtomatik ravishda muhokama qilishga imkon beruvchi protokollar.



1-rasm. IPSec protokoli arxitekturasi

IPsec asosida ishlaydigan to‘rtta asosiy protokol mavjud:

Internet Protokol Autentifikatsiya Sarlavhasi (IP AH): Internet Protokol Autentifikatsiya Sarlavhasi asosan ma’lumotlar yaxlitligi va transport

darajasidagi himoya xizmatlarini taqdim etadi. AH autentifikatsiya ma’lumotlarini qo‘shish uchun ishlab chiqilgan. U ma’lumotlar yaxlitligi, autentifikatsiya va qayta yuborish (replay) hujumlaridan himoya qilish funksiyalarini taqdim etadi. Biroq, ushbu protokolning kamchiliklaridan biri shundaki, u ma’lumotlarni shifrlamaydi. Qayta yuborishdan himoya qilish funksiyasi ruxsatsiz paket uzatilishiga qarshi himoya qiladi. Yana bir muhim kamchiligi shundaki, u ma’lumotlarning maxfiyligini umuman ta’minlamaydi.

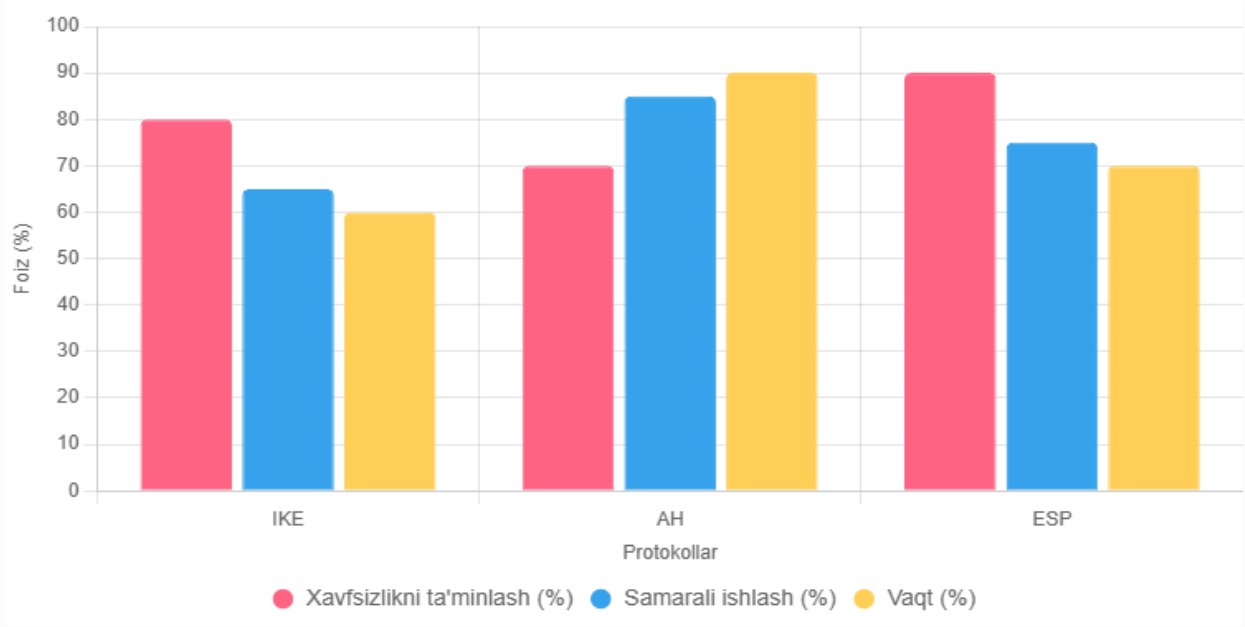
ESP autentifikatsiya, yaxlitlik va maxfiylikni IP paketlarini shifrlash orqali ta’minlaydi. U ma’lumotlarning yaxlitligi, shifrlash va autentifikatsiyasini ta’minlab beradi. Yuklamaning (payload) autentifikatsiyasi ushbu protokolning muhim funksiyalaridan biridir.

Internet Kalitlar Almashinuvi (IKE) — bu ikki tizim yoki qurilmaning ishonchli bo‘lmagan tarmoq orqali xavfsiz aloqa kanalini o‘rnatishiga yordam beruvchi maxsus protokoldir. Ushbu protokol bir nechta kalitlar almashinuvi orqali mijoz va server o‘rtasida xavfsiz tunnel yaratadi, bu orqali ular shifrlangan ma’lumot almashishlari mumkin bo‘ladi. Ushbu tunnelning xavfsizligi Diffie-Hellman kalitlar almashinuvi uslubiga asoslangan, bu esa keng qo‘llaniladigan xavfsizlik texnikasidir.

IPSec protokoli ISAKMP — IKE protokolining tarkibiy qismi bo‘lib, kalitlarni yaratish, autentifikatsiya va xavfsizlik assotsiatsiyasini kelishish uchun ishlatiladi. Bu xavfsiz ma’lumot almashinuvi uchun asosiy parametrlarni belgilovchi asosiy ramkadir. Boshqacha aytganda, ushbu protokol ikki tizim qanday qilib bir-biri bilan xavfsiz aloqa o‘rnatishini belgilaydi. Har bir xavfsizlik assotsiatsiyasi bir yo‘nalishdagi aloqani ifodalaydi: bir hostdan boshqasiga. Xavfsizlik assotsiatsiyasi kriptografik algoritm, IPsec rejimi, shifrlash kaliti va boshqa zarur parametrlardan iborat bo‘ladi.

IPsec qo‘llanilishi: IPsec — bu sezgir ma’lumotlarni himoya qilish va ularni xavfsiz uzatish uchun qo‘llaniladigan xavfsizlik protokoli bo‘lib, moliyaviy operatsiyalar, tibbiy yozuvlar, korporativ aloqa kabi sohalarda keng qo‘llaniladi. IPsec, ayniqsa, virtual shaxsiy tarmoqlar (VPN) uchun ishlatiladi, bunda IPsec tunneli ikkita nuqta yoki qurilma o‘rtasidagi barcha ma’lumotlarni shifrlashga yordam beradi.Shuningdek, IPsec ilova darajasidagi ma’lumotlarni kuchli shifrlash va marshrutizatorlar orqali Internet orqali yuborilayotgan marshrutlash ma’lumotlarini yuqori darajada himoya qilishda yordam beradi. Faqat autentifikatsiyani ta’minlash, lekin shifrlamaslik imkoniyati IPsec’ning foydali jihatlaridan biridir.

Agar IPsec ishlatilmasa, OSI modelining ilova yoki transport qatlamlarida yuqori darajadagi shifrlash bilan ma’lumotlarni xavfsiz tarzda uzatish mumkin. Ilova qatlamida bu ishni HTTPS (Hypertext Transfer Protocol Secure) bajaradi. Transport qatlamida esa TLS (Transport Layer Security) protokoli muhim rol o‘ynaydi. Biroq, ushbu yuqori qatlamlarda autentifikatsiya va shifrlash amalga oshirilganda, ma’lumotlarning ochilib qolish xavfi ortadi.



3.3-rasm. IKE, AH, ESP protokollarini orqali jarayonlarni taqqoslash

IPsec afzalliklari:

IPsec tarmoq qatlami darajasida xavfsizlikni ta’minlaydi va ilovalardan mustaqil ishlaydi.

Ma’lumot almashinuvi jarayonida maxfiylikni ta’minlaydi.

Ilovalardan mustaqil bo‘lib, tarmoq qatlamida bevosita amalga oshiriladi.

IPsec kamchiliklari:

IPsec keng doiradagi kirish imkonini beradi; bitta qurilmaga ruxsat berilsa, boshqa qurilmalar ham tarmoqqa kira olishi mumkin.

Ko‘p hollarda turli dasturiy ta’minotlar bilan mos kelmaslik muammolari yuzaga keladi.

IPsec ko‘p holatlarda yuqori darajadagi CPU resurslarini talab qiladi.

Xulosa

Xulosa o‘rnida quyidagilarni keltirish mumkin:

- Tarmoq xavfsizligi uchun IPsec prortokoli eng yaxshi yexhim hisoblanadi;
- Xavfsizlik darajasi va ishlash samaradorligi juda yuqori;
- Qisqa vaqtda ishlash imkoniyati.