XAVFSIZ TARMOQ TRAFIGINI UZATISH XUSUSIYATLARI

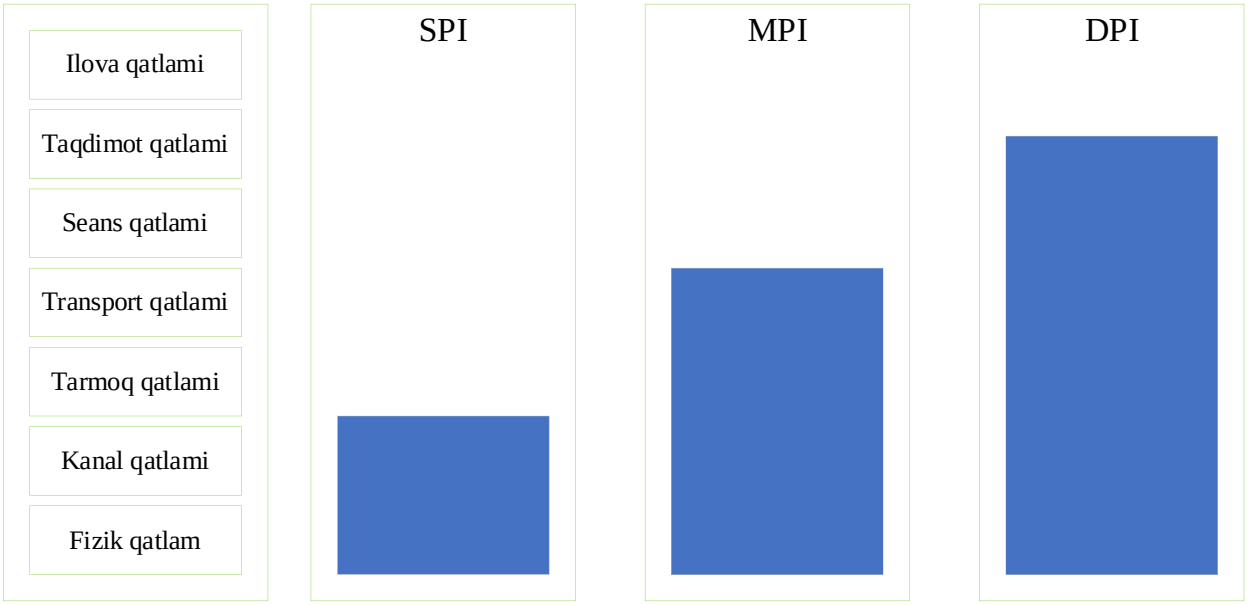
Abdujapparova Mubarak Baltabaevna
Muhammad al-Xorazmiy nomidagi Toshkent Axborot Texnologiyalari Universiteti
"Telekommunikatsiya injiniringi" kafedrasining mudiri, PhD, dotsenti
Muradova Alevtina Aleksandrovna
Muhammad al-Xorazmiy nomidagi Toshkent Axborot Texnologiyalari Universiteti
"Telekommunikatsiya injiniringi" kafedrasining PhD, dotsenti
Shoysayev Ozodxo'ja Anvarxo'ja o'g'li
Muhammad al-Xorazmiy nomidagi Toshkent Axborot Texnologiyalari Universiteti
"Telekommunikatsiya injiniringi" mutaxasisligi magirtranti
(shoysayevozodxoja21@gmail.com)

Tarmoq texnologiyalarining rivojlanishi, tarmoq orqali uzatiladigan ma'lumotlar hajmining ko'payishi va ko'plab yangi tarmoq protokollarining (shu jumladan yopiq protokollar) joriy etilishi tufayli tarmoq trafigini tahlil qilish tobora dolzarb bo'lib bormoqda. Amaliy qo'llashning asosiy yo'nalishlari quyidagilardan iborat:

- tarmoq ishidagi muammolarni aniqlash;
- tarmoq protokollarini sinovdan o'tkazish (tuzatish);
- tarmoq hujumlarining oldini olish;
- trafik sinflashtirilishi.

Quyida paketli kommutatsiya tarmoqlari ko'rib chiqiladi. Amaliy tahlil muammolarini hal qilish, asosan, paketlardagi tarmoq protokoli sarlavhalarini tahlil qilish va uzatilgan ma'lumotlar oqimini tiklashga tayanadi.

OSI modelining turli darajalariga tegishli tahlil qilingan protokol sarlavhalari soniga ko'ra, tahlil qilishning uchta asosiy sinfi ajratiladi (1-rasm): yuzaki (SPI – Shallow Packet Inspection), o'rta (MPI – Medium Packet Inspection) va chuqur (DPI – Deep Packet Inspection).

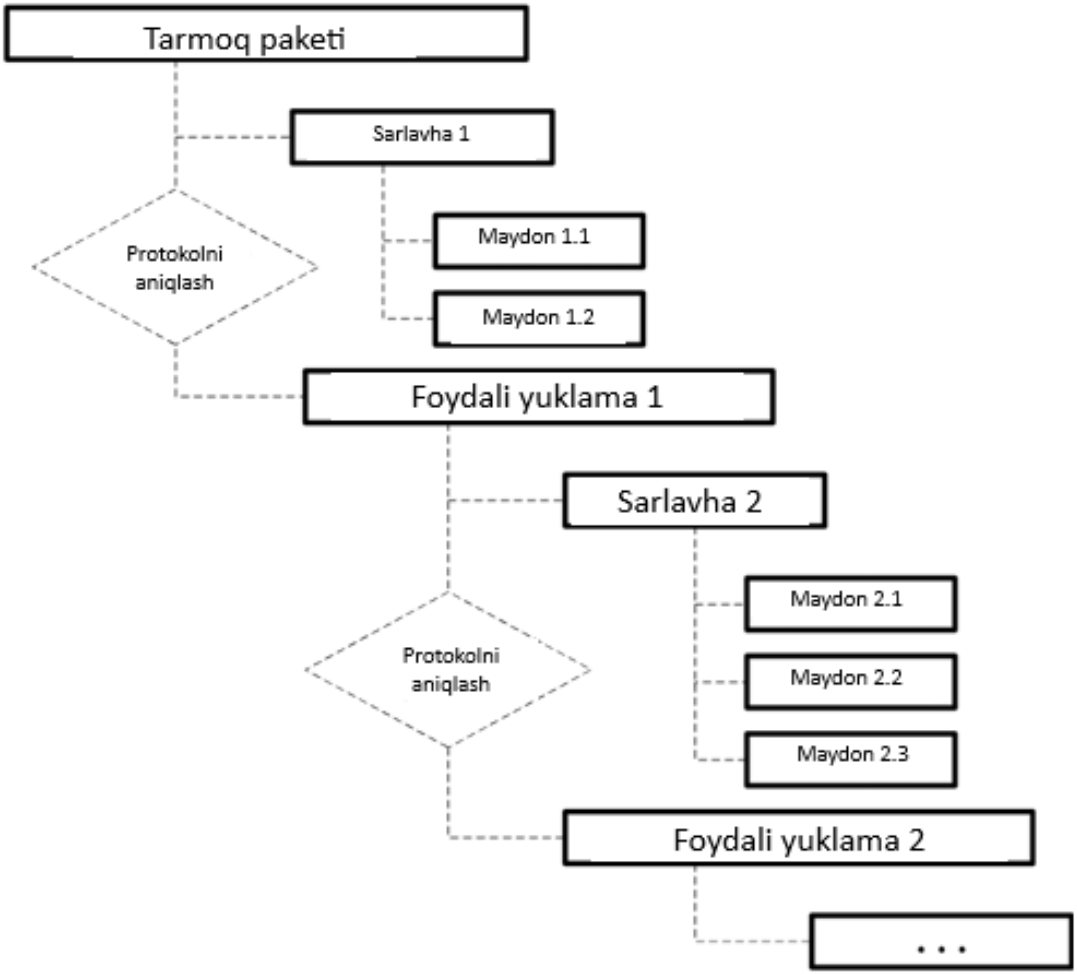


1-rasm. Tarmoq paketlarini tahlil qilish sinflari

"Yuzaki" darajasidagi analizatorlar asosan oddiy xavfsizlik devorlarini o'z ichiga oladi: ma'lum bir paketni blokirovka qilish qarori odatda taqiqlangan IP manzillar va port raqamlari ro'yxatiga muvofiq qabul qilinadi.

"O'rta" darajaga tegishli vositalar uzatiladigan ma'lumotlarning formati haqidagi ma'lumotlardan foydalangan holda trafikni filtrlash, shuningdek jo'natuvchini to'liqroq (alohida IP-manzil bilan solishtirganda) mahalliylashtirish imkonini beradi. Qoida tariqasida, bunday vositalar Internetga kirish provayderi va ichki tarmoq o'rtasida vositachi (ilova proksi) vazifasini bajaradi.

DPI tizimlari birinchi navbatda tarmoq aloqalarida ishtirok etuvchi ilovalarni aniqlash uchun mo'ljallangan. Shuning uchun, "chuqur" tahlil barcha darajadagi tarmoq paketlari tarkibini tahlil qilishni o'z ichiga oladi. Aniqroq identifikatsiya qilish uchun DPI vositalari qo'shimcha ravishda ma'lum tarmoq ilovalari va/yoki protokollariga xos bo'lgan bilvosita atributlardan foydalanishi mumkin. Buning uchun, xususan, statistik tahlil usullari qo'llaniladi.



2-rasm. Paketdagi protokol sarlavhalarini ajratish va tahlil qilish

Har bir tarmoq paketi boshqaruv axboroti va foydali yuklamadan iborat. Bundan keyin “paket” atamasi universal atama sifatida freym, datagramma, tegishli tarmoq protokollarining segmenti kabi tushunchalarni umumlashtirish uchun ishlatiladi. Tahlil qilish jarayonida protokol sarlavhalari paketda ajratiladi va ulardagi maydonlarning qiymatlari tahlil qilinadi. Sarlavhaning tuzilishi spetsifikatsiya bilan belgilanadi, foydali yuklama esa o'zboshimchalik bilan tashkil etilgan ma'lumotlarni o'z ichiga olishi mumkin, garchi u odatda keyingi yuqori darajadagi protokol paketi bo'lsa: tahlil qilishni davom ettirish uchun siz uning qanday protokol ekanligini aniqlashingiz kerak (2-rasm).

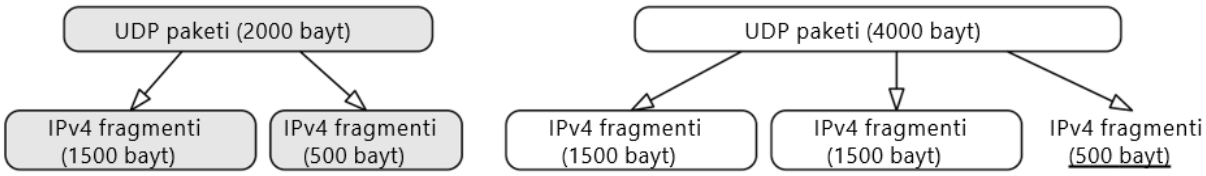
OSI modeliga ko'ra, paketning tarmoq protokoli sarlavhalari stekni tashkil qiladi va qoida tariqasida bir-birini tabiiy tartibda - past darajadan yuqori darajagacha kuzatib boradi. Biroq, tunnel ulanishlarini tashkil qilishda ushbu tartibni buzish mumkin - masalan, IPv4 paketlarini (tarmoq qatlami) UDP protokol paketlari [20] (transport qatlami) ichida uzatishda. Tunnel protokollari

hozir keng tarqalgan: xususan, ular virtual xususiy tarmoqlarni tashkil qilish uchun ishlatiladi. Umumiy holda, har qanday konfiguratsiyadagi tunnelni qurish mumkin: xususan, bitta tunnel boshqasiga joylashtirilishi mumkin. Tunnel trafigini tahlil qilish tarmoq analizatori tomonidan qo'llab-quvvatlanishi kerak.

Holat saqlangan va saqlanmagan protokollar mavjud. Saqlangan holat 0protokoli spetsifikatsiyasining majburiy qismi tegishli avtomat holatlar (Protocol State Machine) hisoblanadi. Real vaqtda tahlilni amalga oshirayotganda, joriy holatning xususiyatlarini saqlash kerak bo'lgan ulanishlar soni cheksiz o’sishi mumkin.

Shuning uchun analizator o'zi uchun mavjud resurslarni taqsimlashni moslashuvchan boshqarishi kerak.

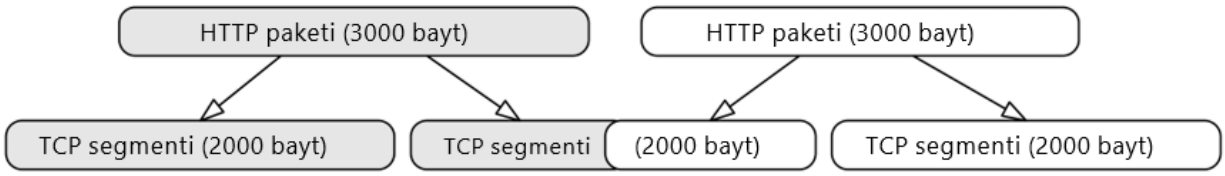
Tarmoq protokolining muhim xarakteristikasi MTU (Maximum Transmission Unit) - bitta paket ichida uzatilishi mumkin bo'lgan ma'lumotlarning maksimal hajmi hisoblanadi. IPv4 uchun MTU qiymati 65535. Amalda IPv4 paketlari odatda Ethernet freymlarida inkapsullanganligi sababli, natijada MTU qiymati tarmoq uskunasi tomonidan qo'llab-quvvatlanadigan Ethernet standartining o'ziga xos versiyasiga muvofiq aniqlanadi. MTU dan kattaroq ma'lumotlar bloklari uchun parchalanish amalga oshiriladi: jo'natuvchi blokni maqbul o'lchamdagi qismlarga ajratadi, shundan so'ng har bir qism alohida paketning bir qismi sifatida uzatiladi. Shuning uchun qabul qiluvchi defragmentatsiyani amalga oshirishi: alohida olingan qismlardan asl blokni tiklashi kerak. IPv4 protokoli uchun oxirgi fragment MF (More Fragments) tashlab yuborilgan bayroq bilan aniqlanadi: u keyingi PDU (Protocol Data Unit - uzatish birligi) ma'lumotlarini o'z ichiga olmaydi (3-rasm).



3-rasm. IPv4 segmentatsiyasiga misol

TCP protokoli holatida (4-rasm), ma'lum bir PDU uchun "oxirgi" segmentning norasmiy belgisi PSH bayrog'i hisoblanadi, ammo bu segment

odatda keyingi uzatish blokining ma'lumotlarini o'z ichiga oladi - chegaralarni aniqlash muammosi paydo bo'ladi.



4-rasm. TCP segmentatsiyasiga misol.

Chuqur tahlil qilish uchun quyidagilar zarur:

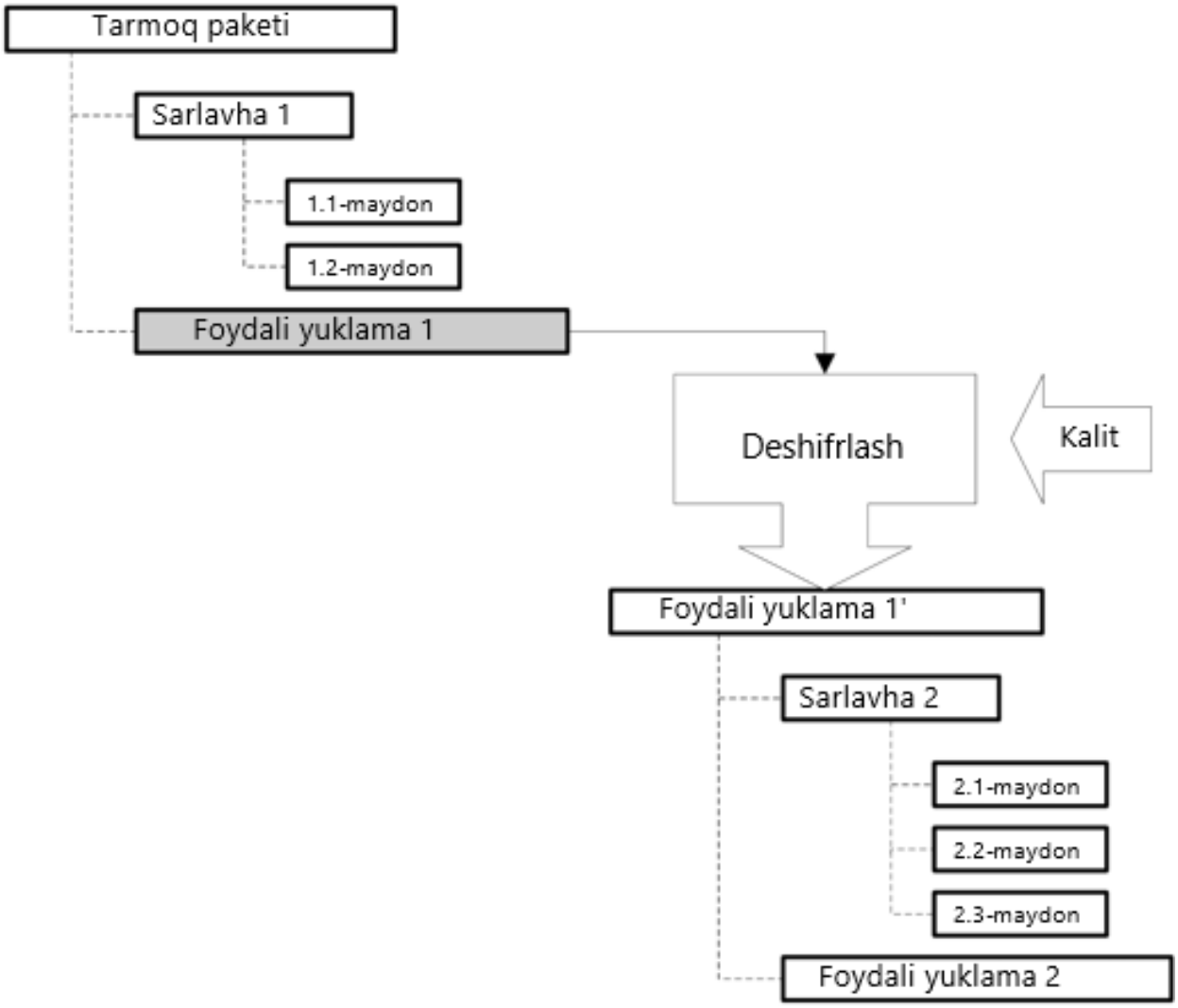
- paketlarning asl tartibini tiklash;
- yuqoridagi PDU chegaralarini aniqlash.

Ulanish xavfsizligini ta'minlash uchun ba'zi protokollar ma'lumotlarni shifrlangan shaklda uzatishni talab qiladi (masalan, TLS protokollar oilasi). Shifrlangan ma'lumotlarni tahlil qilish uchun avvalo foydalanuvchi tomonidan taqdim etilgan kalit yordamida shifrini ochish (5-rasm): analizatorda tahlil qilish uchun yetishmayotgan ma'lumotlarni qo'shish kerak.

Trafikni tahlil qilishda, tahlil qilish xatolari muqarrar ravishda yuzaga keladi. Xato ostida tahlil qilish protokol spetsifikatsiyasi o'rtasidagi nomuvofiqlikni anglatadi (kod, tahlil qilish) va ma'lumotlar ushbu spetsifikatsiyaga muvofiq tahlil qilinadi. Tahlil xatolarining sabablari turlicha:

- hujjatlashtirilmagan protokol imkoniyatlari;
- tarmoqni uzatishda ma'lumotlarning buzilishi;
- analizator kodidagi xatolar.

ISSN 3060-4567



5-rasm. Tashqi kalit yordamida ma'lumotlarni deshifrlash

Tahlil xatolar osongina lokalizatsiya qilinishi va takrorlanishi kerak. Agar duch kelgan xato muhim bo'lmasa, tahlilni davom ettirish kerak.

FOYDALANILGAN ADABIYOTLAR RO'YHATI

[1] Mike Cloppert. An Overview Of Protocol Reverse-Engineering. https://digitalforensics.sans.org/blog/2012/07/03/an-overview-of-protocol-reverse-engineering

[2] IETF RFC 791. J. Postel. Internet Protocol, September 1981

[3] Antonios Atlasis. Fragmentation (Overlapping) Attacks One Year Later, Troopers 13 – IPv6 Security Summit, 2013

[4] IETF RFC 793. J. Postel. Transmission Control Protocol, September 1981

[5] Judy Novak, Steve Sturges. Target-Based TCP Stream Reassembly, 2007

ISSN 3060-4567

[6] Jon C. R. Bennett, Craig Partridge, Nicholas Shectman. Packet reordering is not pathological network behavior // IEEE/ACM Transactions on Networking (TON) archive, Volume 7 Issue 6, Dec. 1999, Pages 789-798