ISSN (E): 2181-4570 ResearchBib Impact Factor: 6,4 / 2024 SJIF 2024 = 5.073/Volume-3, Issue-1

TARMOQ TRAFIGINI SHIFRLAYDIGAN ETHERNET KARTASIGA INTEGRATSILANUVCHI APPARAT MAJMUASINING ARXITEKTURASINI ISHLAB CHIQISH MASALALARI

O‘zbekiston Respublikasi Mudofaa Vazirligi *Axborot-kommunikatsiya texnologiyalari va aloqa harbiy instituti*
Shoxruh Erkin o‘g‘li Alimardonov
shohruhalimardonov1202@gmail.com

ANNOTATSIYA*: Ushbu maqola tarmoq trafigini shifrlaydigan Ethernet kartasiga integratsilanuvchi apparat majmuasining arxitekturasini ishlab chiqish TCP/IP protokoli stekiga asoslangan paketli kommutatsiyalangan kompyuter tarmog‘ining (Ethernet) trafikni boshqarish to‘g‘irisida. Ethernet kartasi texnologiyasidan foydalanishning bugungi kundagi ahamiyati: tarmoq trafigini shifrlaydigan Ethernet kartasi arxitekturasini shakllantirish va kartaga integratsiyalovchi apparat majmuasini yechimlarga bag‘ishlangan.*

Hozirgi kunda internetga (vertual olamga) bo‘lgan talablar ortib borayotganligini inobatga olgan holda internetda ma’lumotlarni xavfsizligini ta’minlashni tashkil qilish kechiktirib bo‘lmaydigan dolzarb muammolardan biriga aylanib bormoqda. Internetning rivojlanishi natijasida dunyoda axborotni tarqatish va foydalanishda sifat o‘zgarishlari sodir bo‘lmoqdi. Internet foydalanuvchilari arzon va qulay kommunikatsiyaga ega bo‘lib bormoqdalar. Korxonalar Internet kanallaridan jiddiy tijorat va boshqaruv axborotlarini uzatish imkoniyatlariga qiziqish bildirishmoqdalar, ammo internetning qurilishi prinsipi ayrim foydalanuvchilarga axborotni o‘g‘irlash yoki atayin buzish imkoniyatini yaratdi. Odatda TCP/IP protokollar va standart Internet-ilovalar (e-mail, Web, FTP) asosida qurilgan korporativ va idora tarmoqlari suqilib kirishdan kafolatlanmaganlar shu sababdan bizda kriptografik himoyalanishga bo‘lgan talab kuchaydi. Internet tarmog‘ida ma’lumotlarni himoyalash bugungi kunda axborot kommunikatsiya texnologiyalari sohasining dolzarb masalalaridan biri hisoblanadi.

ANNOTATION: *This article is about the development of the architecture of the hardware complex integrated into the Ethernet card that encrypts network traffic and the*

ISSN (E): 2181-4570 ResearchBib Impact Factor: 6,4 / 2024 SJIF 2024 = 5.073/Volume-3, Issue-1

traffic management of the packet-switched computer network (Ethernet) based on the TCP/IP protocol stack. The importance of using Ethernet card technology today: the formation of the architecture of the Ethernet card that encrypts network traffic and the solutions of the hardware complex integrated into the card are devoted to.

Nowadays, taking into account the increasing demands on the Internet (virtual world), the organization of ensuring data security on the Internet is becoming one of the urgent problems that cannot be postponed. As a result of the development of the Internet, qualitative changes have occurred in the distribution and use of information in the world. Internet users are becoming more and more affordable and convenient for communication. Enterprises are interested in the possibility of transmitting serious commercial and management information via Internet channels, but the principle of the Internet's construction has created the opportunity for some users to steal or deliberately damage information. Corporate and office networks, which are usually built on the basis of TCP/IP protocols and standard Internet applications (e-mail, Web, FTP), are not guaranteed against intrusion, which is why the demand for cryptographic protection has increased. Data protection on the Internet is one of the current issues in the field of information and communication technologies today.

Kalit so‘zlar: uyali aloqa, *GSM standarti, e-mail, Web, FTP, TCP/IP protokoli, LAN, OSI tarmoq modeli, MAC ramkalari, IEEE 802.1D shaffof ko‘prik, ICMP Redirect, User Datagram Protocol, Transmission Control Protocol, MS-CHAP2 autentifikatsiyasi, Point-to-Point Tunneling Protocol (PPTP), AES (Kengaytirilgan shifrlash standarti) simmetrik blok, IPsec (IP xavfsizligi), OpenSSL kripto kutubxonasi, GNU General Public License (GNU General Public License) ostida tarqatiladigan OpenVPN buzib kirishiga olib kelishi mumkin.*

Keywords: *cellular communication, GSM standard, e-mail, Web, FTP, TCP/IP protocol, LAN, OSI network model, MAC frames, IEEE 802.1D transparent bridging, ICMP Redirect, User Datagram Protocol, Transmission Control Protocol, MS-CHAP2 authentication, Point-to-Point Tunneling Protocol (PPTP), AES (Advanced Encryption Standard) symmetric block, IPsec (IP security), OpenSSL crypto library, OpenVPN distributed under the GNU General Public License (GNU General Public License) can lead to hacking.*

Axborot-kommunikatsiya texnologiyalari davlatlarning iqtisodiy raqobatbardoshligi va milliy xavfsizligi darajasiga sezilarli ta'sir ko‘rsatib bormoqda.

ISSN (E): 2181-4570 ResearchBib Impact Factor: 6,4 / 2024 SJIF 2024 = 5.073/Volume-3, Issue-1

Davlat idoralari va xususiy korxonalarning tarmoq infratuzilmalarining aksariyat hollarida Ethernet texnologiyasida tashkil etilgan va TCP/IP protokoli stegi asosida ishlaydigan va butun dunyoda keng tarqalgan global Internet tarmog‘iga ulangan. Biroq, bu texnologiyalar, birinchi navbatda, “qattiq” mantiqqa asoslangan turli darajadagi o‘zaro ta'sirning protokollari algoritmlari bilan bog‘liq bir qator zaifliklarga ega.

Korporativ kompyuter tarmoqlarida (jumladan, geografik jihatdan taqsimlangan) aloqa kanallarining yuklanishini optimallashtirish zarurati zamonaviy IT texnologiyalarining ustuvor vazifalaridan biri bo‘lib kelmoqda. Yana bir muhim jihat - ma'lumotlarni uzatish jarayonini himoya qilish. Axborot xavfsizligi darajasi transportni boshqarish usullarining samaradorligi natijasidir. Ushbu maqsadlarga erishish uchun kompyuter tarmoqlari harakatini boshqarishning maxsus usullari ishlab chiqilmoqda.

Shunday qilib, korporativ kompyuter tarmoqlarining trafikni ishonchli ishlashini ta'minlash nuqtai nazaridan boshqarish masalalari V.M.Vishnevskiy, V.V.Rykov, V.A.Ivnitskiy, S.N.Verbitskiy, Kelli F.P., Korilis Ya, Altman E., Tyorner S.larning ishlarida ko‘rib chiqilgan. Biroq, bu tadqiqotlarda inson omili, real tizimlarda yuzaga keladigan insayder tahdidlar hisobga olinmagan.

2009 - yildan beri mahalliy tarmoqlarda (LAN) trafikni boshqarish algoritmlari va usullarini rivojlantirishning asosiy tendentsiyasi axborot xavfsizligini ta'minlash bilan imzo, xulq-atvor, kombinatsiyalangan usullardan foydalangan holda anomal tarmoq trafik faolligini aniqlash texnologiyalari sohasidagi tadqiqotlar o‘tkazilib borilgan. Ushbu yo‘nalishda erishilgan natijalar, quyidagi olimlarning asarlarida chop etilgan: Ajmuxamedov I.M., Gamayunov D.Yu., Kachalin A.I., Marienkov, A.N., Selin R.N., P.Lippmann, R.Kvitt, M.Szmit, L Chang va boshqalar. Ushbu usullar malakali mutaxassislarning yordamiga muhtoj bo‘lgan qat'iy mantiq asosida ishlaydi.

Tarmoq trafigining o‘ziga o‘xshashligi, shuningdek modernizatsiya masalalari tekshirish va filtrlash uchun statistik ma'lumotlarni to‘plash uchun asboblar to‘plami Tarmoq paketlarini mazmuniga ko‘ra (ingliz. Deep Packet Inspection, qisqartma DPI) Meretukov Sh.T., Gabdrahmanov A.A., Skuratov A.K. asarlarida taqdim etilgan.

Ushbu usullar kriptografik protokollarga ega bo‘lgan haqiqiy tizimlarda ishlashga yoki ularning turini yashirish uchun paketlarning elementar parchalanishiga qaratilgan emas (masalan, Tor - tarmoqlarida tashkil etilgan). Bu holatlar aloqa kanallarini yuklashni optimallashtirish va axborot xavfsizligi (AK) darajasini oshirish, shu

ISSN (E): 2181-4570 ResearchBib Impact Factor: 6,4 / 2024 SJIF 2024 = 5.073/Volume-3, Issue-1

jumladan, inson omilini minimallashtirish imkonini beruvchi kompyuter tarmoqlari trafigini intellektual moslashuvchan boshqarishning yangi usullarini ishlab chiqishni taqozo etadi.

Shunday qilib, Ethernet kartasiga integratsiyalangan apparat majmuasi ochiq tarmoq orqali o‘tkazilgan ulanish bo‘lib, u orqali virtual tarmoqning kriptografik himoyalangan axborot paketlari uzatiladi. Axborotni ushbu tarmoq trafigini apparat bo‘yicha uzatilishi jarayonidagi himoyalash quyidagi vazifalarni bajarishga asoslangan:

- o‘zaro aloqadagi taraflarni autentifikatsiyalash;
- uzatiluvchi ma’lumotlarni kriptografik berkitish (shifrlash);
- yetkaziladigan axborotning haqiqiyligini va yaxlitligini tekshirish.

Global Internet tarmog‘i modullik va ochiqlik tamoyillari asosida qurilgan. Bir tomondan, u har bir darajadagi raqobat va avtonom parallel rivojlanishni keltirib chiqaradigan taraqqiyotga yordam beradi, lekin boshqa tomondan, u zararli harakatlar uchun bilim bazasini ta'minlaydi.

TCP/IP protokoli stegi OSI tarmoq modeliga mos keladi (ochiq tizimlar o‘zaro ulanishining asosiy mos yozuvlar modeli). LAN trafigini boshqarish vazifasida bunga arziydi jismoniy qatlam texnologiyalaridan mavhum: aloqa kanallari, signallarni kodlash va multiplekslash (chunki bu alohida tadqiqot yo‘nalishi). Har bir darajada ma'lumotlar mustaqil ma'lumotlarni uzatish birliklari - datagramlar shaklida uzatiladi.

Ma'lumotlar havolasi sathida datagrammalar MAC ramkalari bilan ifodalanadi va uning vazifalari o‘zaro ta'sir qiluvchi tugunlar o‘rtasida mantiqiy aloqani o‘rnatish, qabul qiluvchi va ma'lumot uzatuvchi tezligini joriy ulanish doirasida moslashtirish, shuningdek, xatolarni aniqlash va tuzatishga qisqartiriladi. Tarmoq qurilmalari (masalan, kalitlar) freymlarni yo‘naltirish uchun IEEE 802.1D shaffof ko‘prik algoritmidan foydalanadi. Noxush suratga olish rejimida ishlaydigan xost unga ulangan segmentlardagi barcha trafikni skanerlaydi, tarmoq topologiyasini tekshiradi va Forwarding Database ni kompilyatsiya qiladi. U MAC manzillari va portlarining xaritasini yozib oladi. Agar kadrni oldinga siljitish paytida tegishli yozuv topilmasa, u holda translyatsiya manba portidan tashqari barcha portlarga amalga oshiriladi. Ushbu algoritm uchun elementar tahdid bu translyatsiya manzili bo‘lgan kadrlarni intensiv ishlab chiqarish orqali dasturiy ta'minot yoki apparatdagi nosozliklarni soxtalashtiradi. IEEE 802.1D algoritmiga muvofiq kalit soxta trafikni barcha portlarga uzatadi va translyatsiya bo‘ronini yaratadi. Berilgan darajadagi tarmoq tugunlarining namunaviy

ISSN (E): 2181-4570 ResearchBib Impact Factor: 6,4 / 2024 SJIF 2024 = 5.073/Volume-3, Issue-1

birliklari ushbu zaiflikni bartaraf etmaydigan intensivlik chegarasini belgilashga imkon beradi. Ushbu parametrning qiymati dinamik ravishda hisoblab chiqilishi va aqlli moslashuvchan algoritmlar tomonidan o‘rnatilishi kerak bo‘ladi. Routerlar translyatsiya bo‘ronlarini bartaraf etishga qodir, ammo qo‘shimcha funktsiyalarsiz (masalan, IP-bog‘lash, Port-xavfsizlik) ular FDB jadvalini soxtalashtirishdan himoya qila olmaydi, shu bilan birga ular o‘zlarining keng doiradagi zaifliklariga ega.

Ushbu algoritmlar xost buferining to‘lib-toshgan hujumlariga qarshi himoyasizdir. Buzg‘unchining harakatlari TOS (xizmat turi) bitlarini, qayta aloqani boshqarish harakatlari (dastlab sniffer tomonidan o‘rganilgan) va manzillarni soxtalashtirishda samaraliroq.

Tarmoq darajasida quyi tarmoq operatsiyalari boshqariladi: eng qisqa marshrutlarni topish, kommutatsiya va marshrutlash, muammolarni tashxislash, mantiqiy manzillar va nomlarni jismoniy (IP va DNS dan MAC manzillariga) tarjima qilish. Ushbu daraja doirasida quyidagi protokollar asosiy hisoblanadi:

I.IP (inglizcha Internet Protocol) - internet bilan ishlash protokoli;

II.ICMP (English Internet Control Message Protocol) - xatolar haqida xabar berish uchun foydalaniladigan Internetni boshqarish xabar protokoli;

III.ARP (Address Resolution Protocol) va teskari RARP - IP va MAC manzillarini hal qilish protokollari;

IV.RIP2 (English Routing Information Protocol v2) - ikkinchi versiyaning marshrutlash ma'lumotlari protokoli;

V.OSPF (Open Shortest Path First) Dijkstra algoritmidan foydalangan holda havolalarni kuzatish algoritmlariga asoslangan dinamik marshrutlash protokoli.

Ushbu protokollar algoritmlarining qat'iy mantig‘i har xil turdagi hujumlar uchun keng qamrovli zaifliklarni ta'minlaydi: noto‘g‘ri ARP javoblari, noto‘g‘ri yo‘riqnoma o‘rnatish, noto‘g‘ri konfiguratsiya parametrlarini o‘rnatish, marshrutlash protokollarining ishlamay qolishi, o‘zini taqlid qilish va boshqalar.

ISSN (E): 2181-4570 ResearchBib Impact Factor: 6,4 / 2024 SJIF 2024 = 5.073/Volume-3, Issue-1

Birinchi holda, tajovuzkor bir xil IP tarmog‘ida joylashgan "A" va "B" tugunlari orasidagi trafikni ushlab turish uchun ARP protokolidan foydalanadi. Soxta ARP xabarlari shunday yuboriladiki, hujum qilingan xostlarning har biri tajovuzkorning MAC manzilini suhbatdoshining manzili bilan izohlaydi

(1.1-rasmda ko‘rsatilgan).

1.1-rasm. Soxta ARP javoblari bilan hujum

ARP hujumlarini aniqlash uchun tizim ma'muri barcha tarmoq tugunlarining MAC va IP manzillari ma'lumotlar bazasini saqlashi, IP-bog‘lash (MAC va IP-manzillar) va Port-xavfsizlik (MAC manzillarini portlarga bog‘lash) funktsiyalari bilan qimmatroq L2 kalitlaridan foydalanishi kerak. Shuningdek, faol trafikni aniqlash dasturidan foydalaniladi. Ammo bu harakatlar tahdidni bartaraf etmaydi, chunki kalitlarning IP-MAC-portiga ulanishi ikkita ish rejimini o‘z ichiga oladi: ARP (sukut bo‘yicha) va kirishni boshqarish ro‘yxati (ACL).

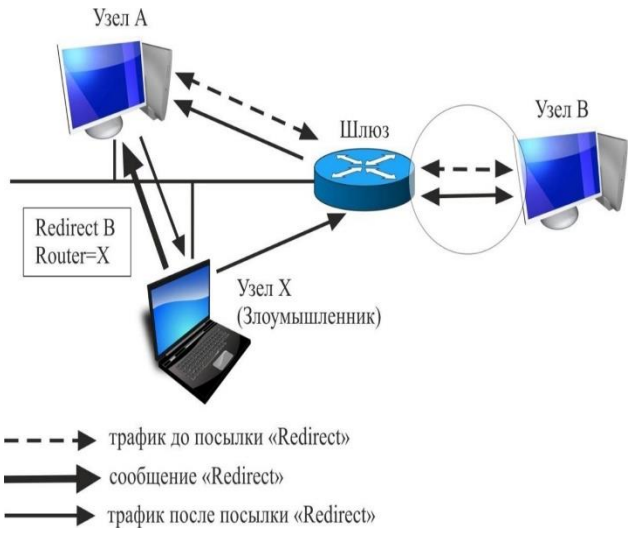
Birinchi holda, agar xaker sniffer kalitni buzish uchun o‘ziga statik manzilni tayinlagan bo‘lsa, filtrlashni tashkil qilish mumkin emas. Ikkinchisida, ACL profili sarflanadi (raqam cheklangan), shuningdek, ACL strategiyasini yaxshilab o‘ylab ko‘rish kerak bo‘ladi.

Soxta yo‘riqnoma hujumi (1.2-rasmda ko‘rsatilgan) tajovuzkor tomonidan ba'zi "A" xostlaridan boshqa tarmoqqa yuborilgan ma'lumotlarni ushlab turish uchun ushbu xost manzilini yo‘riqnoma manzili sifatida majburlash orqali ishlatilishi mumkin. Shunday qilib, "A" xostining trafigi tajovuzkor tugunidan o‘tadi, u ma'lumotlarni tahlil qilgandan va ehtimol o‘zgartirgandan so‘ng, uni haqiqiy routerga jo‘natadi.

Spoofing soxta ICMP Redirect xabarlari yordamida amalga oshiriladi. RFC-1122

ISSN (E): 2181-4570 ResearchBib Impact Factor: 6,4 / 2024 SJIF 2024 = 5.073/Volume-3, Issue-1

ga binoan, bunday xabarlarni qayta ishlash uchun tarmoq tugunlari talab qilinadi.



1.2-rasm. Router hujumini aldash

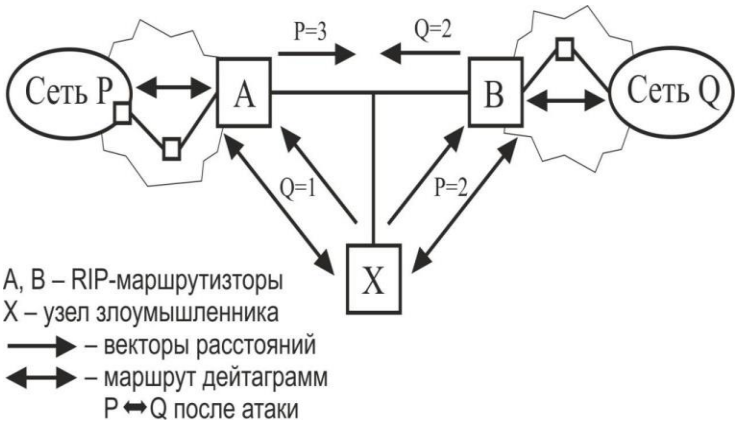
Shuni ta'kidlash kerakki, hatto tarmoq tugunlarida qayta yo‘naltirish xabarlarini qayta ishlashni o‘chirib qo‘yish ham bu zaiflikni har doim ham ishonchli tarzda yopmaydi, chunki operatsion tizimlarda bir qator "teshiklar" mavjud, bunga misol sifatida maxsus bo‘lingan paketni qayta ishlashda ushbu parametrni yoqish mumkin. Ba'zi operatsion tizimlar ushbu sozlamalarni o‘zgartirish imkoniyatini ta'minlamaydi.

Hujum xuddi shunday xostni sozlashda amalga oshiriladi. ICMP Router reklama xabari yoki Dynamic Host Configuration Protocol (DHCP) orqali soxta chegara tugunini kiritish mumkin. Buzg‘unchi tarmoqda soxta DHCP serverini o‘rnatishi mumkin. Jabrlanuvchi xostning DHCP mijozi translyatsiya qilingan DHCP qidiruv xabarini yuboradi, unga barcha DHCP serverlari o‘zlarining DHCP takliflarini yuboradilar va birinchisi qabul qilinadi va tasdiqlanadi. Shunga ko‘ra, tarmoq hujumlarini birlashtirib (soxta serverdan paket birinchi o‘rinda turishi uchun) tajovuzkor qurbonni keyingi xakerlik yoki uning qonuniy tarmoqdagi mavjud bo‘lmagan holati uchun butunlay izolyatsiya qilishi mumkin.

Marshrutlash protokollariga hujum qilish korxonaning axborot xavfsizligi AKTga yuqori darajada tahdid soladi. Bu tajovuzkor tomonidan chegara shlyuzi zonasida joylashganida trafikni ushlab turish maqsadida amalga oshiriladi. Kerakli marshrutlarni o‘z tarmoq tuguniga o‘tkazish uchun soxta marshrutlash protokoli xabarlari yuboriladi. Hujumning namunasi 1.3-rasmda ko‘rsatilgan, bu erda xaker ("X" tugun) "P" tarmog‘ining tugunlari va "Q" tarmog‘ining tugunlari o‘rtasida joylashgan va ular orasidagi trafikni ushlab turishni xohlaydi. *1.3-rasm. Marshrutlash rotokollariga hujum*

ISSN (E): 2181-4570 ResearchBib Impact Factor: 6,4 / 2024 SJIF 2024 = 5.073/Volume-3, Issue-1

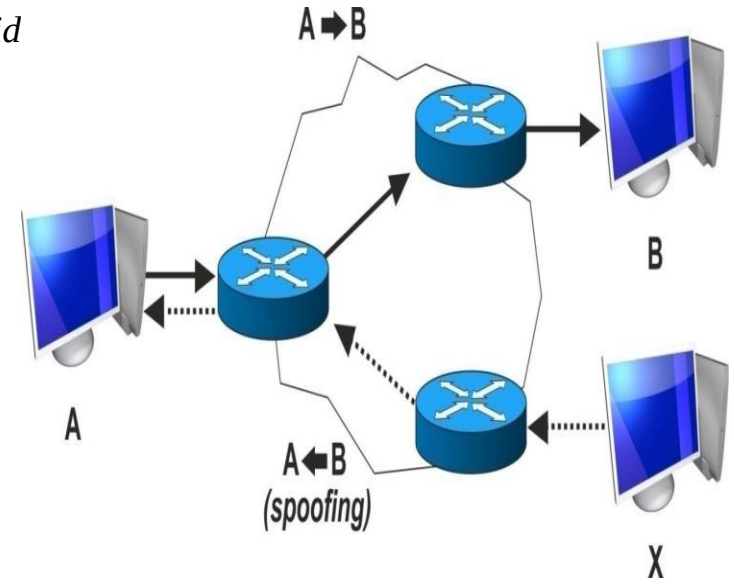
"X" xost RIP-xabarlarni uzatadi: vektor P = 3 "A" tugunidan va vektor Q = 2 "B" tugunidan. Keyin u kam baholangan metrik parametrlarga ega bo‘lgan "A" va "B" tugunlariga xabarlarni yuboradi: mos ravishda Q = 1 va P = 2 vektorlari. TCP/A-MD5 autentifikatsiyasi ushbu tahdidni qisman yumshatadi, ammo marshrutizatorlardagi dasturiy zaifliklar uni ochiq qoldiradi.



O‘zaro ishlaydigan qatlamdan keyin ma'lumotlarni yetkazib berish uchun mas'ul bo‘lgan Transport qatlami keladi. Ushbu darajada eng ko‘p qo‘llaniladigan protokollar - User Datagram Protocol va Transmission Control Protocol. Birinchisi yuqori tezlikdagi ma'lumotlarni uzatishni ta'minlaydi, ikkinchisi esa ishonchli va aniq bog‘langan. TCP Sliding Window Mode parametrlari va qayta aloqa mexanizmlarini osongina o‘zgartirish mumkin xaker, masalan, ikkinchi tugunning buferini to‘ldirish uchun ma'lumotlarni uzatishni tezlashtirish uchun. Qo‘shma hujumlarda desinxronizatsiya va keyinchalik TCP ulanishi ustidan nazoratni qo‘lga kiritish yordamida taqlid qilish qo‘llanilishi mumkin.

Ochiq tsiklli taqlid qilish (1.4-rasmda ko‘rsatilgan) "X" xost "A" va "B" xostlaridan uzoq tarmoqda (hatto ularning chekkasida Internet bilan ishlash segmentida ham emas) bo‘lganida yanada qiziqarli holatni taqdim etadi.

ISSN (E): 2181-4570 ResearchBib Impact Factor: 6,4 / 2024 SJIF 2024 = 5.073/Volume-3, Issue-1



1.4-rasm. Fikr-mulohazasiz taqlid qilish

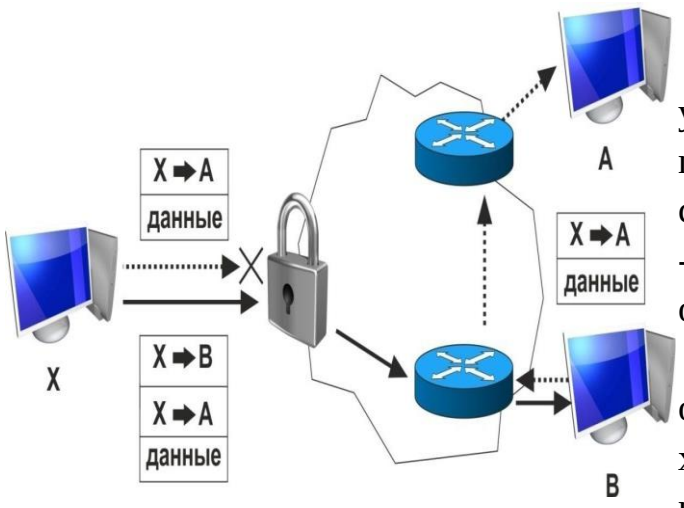
Operatsiya faqat birovning nomidan ma'lumotni bir tomonlama uzatish uchun amalga oshiriladi (masalan, "B" tugunining nomidan).

Bitta tarmoq segmenti doirasida TCP/IP modelining "qattiq" mantig‘ining zaifligi (birinchi navbatda ma'lumotlarni uzatish ishonchliligiga qaratilgan) tufayli TCP ulanishini desinxronizatsiya qilishga hujumdan foydalanish mumkin. Ingliz tilidagi adabiyotlarda ulanish ustidan to‘liq nazorat o‘rnatish uchun taqlid qilish TCP hijacking deb ataladi.

Sinxronizatsiya holatida ma'lumotlarni almashishga urinishlar ACK bo‘ronlari oqimini keltirib chiqaradi va ulanish ishtirokchilari bo‘lgan segmentlar bundan mustasno. Xaker vositachi funktsiyalarini o‘ziga topshiradi.

Ushbu hujumlarning turli xil o‘zgarishlari mavjud: erta, faol, nol va boshqa desinxronizatsiya. Agar marshrutizatorga Protokol maydoni 4 bo‘lgan datagrammalarni va tashqi tarmoqqa parametrlari bo‘lgan datagrammalarni uzatishga ruxsat berilsa, u holda tunnel qurish xavfi mavjud. Masalan, marshrutizator faqat "B" xostiga tashqi xostlar tomonidan datagrammalarni yuborishga ruxsat beradi, qolgan manzillar blokirovka siyosatiga bo‘ysunadi. Xaker "B" tugunidan "A" ga yo‘naltirilgan paketlar uchun o‘rni sifatida foydalanishi mumkin. Buning uchun u "X" dan "B" ga yo‘naltirilgan datagrammani yaratadi, uning Protokol maydoniga 4 qiymati ("IP") qo‘yiladi va kerakli IP datagramma "dan yo‘naltirilgan ma'lumotlar maydoniga kiritilgan. X" dan "A" gacha (1.5-rasmga muvofiq).

ISSN (E): 2181-4570 ResearchBib Impact Factor: 6,4 / 2024 SJIF 2024 = 5.073/Volume-3, Issue-1



1.5-rasm. Tunnel hujumi

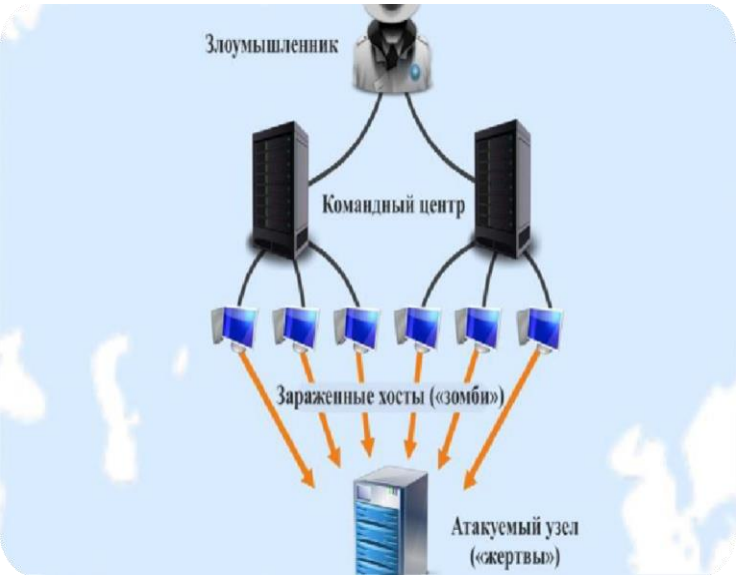
Router filtri ruxsat etilgan B xostiga yuborilgan paketni uzatadi va B hostining IP moduli undan o‘rnatilgan datagrammani chiqaradi, so‘ngra uni aniqlangan manzilga - A xostiga yuboradi. Tunnel qazish operatsiyasi muvaffaqiyatli yakunlandi.

Ilova qatlami protokollarini hisobga olgan holda Microsoft korporatsiyasining xususiy RDP (Remote Desktop Protocol) ni misol qilib keltirish mumkin. Uning vazifasi foydalanuvchilarning terminal ulanish xizmati bilan ishlaydigan server bilan masofaviy ishlashini ta'minlashdan iborat. Mijozlar Windowsning barcha versiyalariga birlashtirilgan. Operatsion tizimlar va dasturiy ta'minotning nomukammalligi kiberjinoyatchilar tomonidan jahon iqtisodiyotiga katta zarar yetkazilishining asosiy sabablaridan biridir. Qo‘llab-quvvatlash uchun tizim xavfsizligi holati dasturiy ta'minot yangilanishlari, "yamalar" chiqariladi. Jarayon takrorlanuvchi va cheksiz bo‘lib, qoida tariqasida, xatoning dastlabki identifikatsiyasiga nisbatan sezilarli kechikish bilan davom etadi.

- zararli. Bu tizimning kutilmagan xatti-harakatlari, ishdan chiqishi, zaifliklar, xatolarni nazarda tutadi. Shunday qilib, MS12-020 xavfsizlik byulletenining chiqarilishi xakerlar tomonidan Internet I2P yashirin tarmoqdagi tematik forumlardagi zaifliklar tavsiflanganidan bir yil o‘tgach sodir bo‘ldi (1.3-betga qarang). Ushbu MS12-020 yamog‘ining bir qismi sifatida ikkita zaiflik yopildi: CVE-2012-0002 (RDP-da RCE) va CVE-2012-0152 (Terminal Serverda DoS), bu maxsus ishlab chiqilgan dastur yordamida masofaviy tizimda o‘zboshimchalik bilan kodni bajarishga imkon beradi. RDP paketi va tarmoq qurtlarini tarqatish.

Zamonaviy kompyuter tarmoqlarida trafikni boshqarish algoritmlari va usullari uchun eng muhim tahdid bu taqsimlangan tarmoq hujumlari, masalan, "Xizmat ko‘rsatishni rad etish" DDoS (Distributed Denial of Service, 1.6-rasmda ko‘rsatilgan).

ISSN (E): 2181-4570 ResearchBib Impact Factor: 6,4 / 2024 SJIF 2024 = 5.073/Volume-3, Issue-1



1.6-rasm. Tarqalgan tarmoq hujumlari (DDoS)

Uning maqsadi hujum qilingan tugunni mavjud bo‘lmagan holga keltirishdir. Ta'kidlash joizki, mavjud himoya va harakatni boshqarish tizimlari mavjud emas uni yagona identifikatsiyalash va yuridik tugunlarning so‘rovlaridan farqlash imkoniyatiga ega.

An'anaviy ravishda xakerning harakatlarini quyidagi bosqichlarga bo‘lish mumkin:

1) tajovuzkor N Internet tugunlarini zararli kod bilan zararlaydi va ularni "zombi kompyuterlar"ga aylantiradi;

2) ularga bir vaqtning o‘zida bitta qurbonga (har qanday serverga) hujum qilish buyrug‘ini beradi, masalan, yarim ochiq tcp ulanishlari taktikasidan foydalangan holda;

3) server xost u bilan aloqa o‘rnatishga harakat qilmoqdami yoki virusli xost uni mavjud holatdan olib tashlayaptimi yoki yo‘qligini aniqlay olmaydi. Ulanish chegaralarini belgilash kerak. Biroq, egasi uchun bu nomutanosib vaqtni talab qiladi va malakali tizim ma'murining aralashuvini talab qiladi.

Natijada, axborot resursi bir muncha vaqt davomida haddan tashqari yuklangan va ruxsat etilgan ulanishlar uchun mavjud emas va, ehtimol, buzilgan. Afsuski, provayder darajasida filtrlash, ulanish chegaralarini o‘rnatish va virusli xostlar manzillarining global qora ro‘yxatini joriy etish har doim ham samarali usullar emas.

2009 yildan beri LAN trafigini boshqarish algoritmlari va usullarini rivojlantirishning asosiy tendentsiyasi axborot xavfsizligini ta'minlash bilan imzo, xulq-atvor, kombinatsiyalangan usullardan foydalangan holda anomal tarmoq trafigi faolligini aniqlash texnologiyalari sohasidagi tadqiqotlar o‘tkaziladi. Bu sohada tadqiqotchilar ilmiy arboblar: Ajmuxamedov I.M., Gamayunov D.Yu., Kachalin A.I., Marienkov, A.N., Selin R.N., P.Lippmann, R. Kwitt, M. Szmit, L. Chang va boshqalar.

Statistik tahlil o‘ziga o‘xshashlik parametrlariga asoslanadi, bu esa uni kirish

ISSN (E): 2181-4570 ResearchBib Impact Factor: 6,4 / 2024 SJIF 2024 = 5.073/Volume-3, Issue-1

tarmoqlari va trafikni yig‘ish provayderlari tomonidan qo‘llaniladigan mavjud DPI texnologiyasidan ajratib turadi. Afsuski, faqat ikkinchisi viruslarni aniqlash va blokirovka qilishning minimal darajasiga, kirish ro‘yxatlarining belgilangan mezonlariga javob bermaydigan ma'lumotlarni filtrlashga qodir.

Ammo kriptografik protokollarning kiritilishi yoki paketlarning turini yashirish uchun elementar parchalanishi (masalan, Tor-tarmoqlarida tashkil etilgani kabi) bilan bu usullar aniq natija bermaydi.

Shu munosabat bilan korxona AKT axborot xavfsizligini ta'minlashda LAN trafigini boshqarish va tarmoq tahdidlariga qarshi turishning yangi usullarini ishlab chiqish zarurati tug‘iladi.

Xavfsiz kanallar orqali trafikni nazorat qilish

Xavfsiz kanal texnologiyasining maqsadi ochiq transport tarmog‘i orqali ma'lumotlarni uzatish xavfsizligini ta'minlashdir. Eng keng tarqalgan foydalanish holati TCP/IP protokoli stekiga qurilgan global Internet tarmog‘idir. Shunday qilib, paketli kommutatsiya tarmoqlarida himoyalangan kanallarning virtual kommutatsiyasi o‘rnatiladi, bu uchta asosiy funktsiyani bajarishni o‘z ichiga oladi:

- abonentlarni o‘zaro autentifikatsiya qilish;
- kanal orqali uzatiladigan xabarlarni ruxsatsiz kirishdan himoya qilish;
- kanal orqali kelayotgan xabarlarning yaxlitligini tasdiqlash.

Xavfsiz kanal standartlarining muhim xususiyati bu protokollar ishlaydigan TCP / IP protokoli stekining model qatlamidir.

1) qo‘llaniladigan (Ilova qatlami) - S / MIME / PGP / HTTPS va boshqalar;
2) transport (inglizcha Transport qatlami) - SSL / TLS / SOCKS va boshqalar;
3) tarmoq (inglizcha Internet qatlami) - IPSec (AH, ESP) va boshqalar;
4) kanal (inglizcha havola qatlami) - PPTP / L2TP / PAP / MS-CHAP va boshqalar.

Ushbu protokollarning algoritmlarida (xulq-atvorning "qattiq" mantig‘i tufayli) va ularning apparat va dasturiy ta'minotini amalga oshirishda zaifliklarning keng doirasi mavjud. Qoidaga ko‘ra, zaifliklar kamida ikki yildan keyin umumiy ko‘rib chiqishga topshiriladi. Masalan, OpenSSL “Heartbeat” va MITM zaifliklari 2012-yilda xakerlarning dolzarb manbalarida I2P yashirin Internet qoplamasi hamda CVE-2014-

ISSN (E): 2181-4570 ResearchBib Impact Factor: 6,4 / 2024 SJIF 2024 = 5.073/Volume-3, Issue-1

0160 va CVE xavfsizlik byulletenlari nashr etilgan.

"Heartbeat" dasturiy ta'minotidagi xatolik xakerga to‘g‘ridan-to‘g‘ri kirishga imkon beradigan Transport Layer Security (TLS)/DTLS (Datagram Transport Layer Security) protokollari uchun Heartbeat kengaytmasi protseduralaridan birida (RFC6520) zarur chegara tekshiruvining yo‘qligi edi. Aloqalari OpenSSL ning zaif versiyasi bilan "himoyalangan" kompyuterlarning operativ xotirasi. Buzg‘unchi TLS serveri va TLS mijozining shaxsiy kalitlarini, cookie-fayllarni, loginlarni, parollarni va server va mijozlar o‘rtasida almashinadigan boshqa ma'lumotlarni osongina hisoblab chiqishi mumkin edi.

Keling, OpenSSL va TLS protokollariga qarshi MITM hujumlarini ko‘rib chiqaylik. SSL/TLS sessiyasi ClientHello/ServerHello xabarlari orqali muzokaralarni boshlaydi. Seans parametrlari o‘rnatiladi: protokol versiyasi va kengaytmalari, kalitlar bilan shifrlash turi, xabarning haqiqiylik kodi, ishga tushirish vektorlari va boshqalar. Kriptografik algoritm tanlash siyosatini o‘zgartirish Change Cipher Spec (CCS) so‘rovi orqali amalga oshiriladi. Standartlarga ko‘ra (RFC 2246, RFC 5246), CCS xavfsizlik parametrlari bo‘yicha muzokaralar olib borilgandan so‘ng qo‘l siqish paytida yuboriladi, lekin xabarning mavjudligini tekshirishdan oldin.

“Fyakunlandi – yuborildi. OpenSSL muzokaralar kutilayotgan CCSni qabul qiladi xavfsizlik sozlamalari. Muvaffaqiyatli hujum uchun global kuzatuvchi nol uzunlikdagi OpenSSL asosiy kalitini qo‘llash uchun ulanishni o‘rnatish vaqtida ikkala tugunga CCS paketini yuboradi. Seans kalitlari null kalit zaifligini meros qilib oladi. O‘tkazilgan ma'lumotlarning shifrini ochish va o‘zgartirish xavfi mavjud. Tarmoq tahdidini xakerlik jargonida amalga oshirish uchun ko‘rib chiqilgan algoritm MITM (O‘rtadagi odam) vositachi hujumi deb ataladi.

OAuth va OpenID avtorizatsiya va autentifikatsiya protokollaridagi xatto 2012-yilda TOR yashirin tarmoqli xakerlar forumlarida tasvirlangan, ammo ekspluatatsiya Van Jing tomonidan rasman 2014-yilning may oyida taqdim etilgan Auth Gmail, Facebook, Twitter yoki Microsoft hisob qaydnomalari yordamida uchinchi tomon xizmatlariga "o‘tish" orqali ro‘yxatdan o‘tish obuna bo‘lish uchun yaratilgan. OpenID protokolining vazifasi shaxsiy foydalanuvchi ma'lumotlarini taqdim etish bilan uchinchi tomon portallarida markazlashtirilmagan autentifikatsiyadan iborat. Yashirin qayta yo‘naltirishdan foydalanib, soxta qonuniy dasturdan provayderga so‘rov yuboriladi. Aslida, boshqa manbaga yashirin yo‘naltirish URL manzilidagi redirect_uri parametrini

ISSN (E): 2181-4570 ResearchBib Impact Factor: 6,4 / 2024 SJIF 2024 = 5.073/Volume-3, Issue-1

almashtirish orqali amalga oshiriladi. Maxfiy foydalanuvchi ma'lumotlarining tarqalishi va maqsad tugunlarining buzilishi xavfi mavjud.

Alohida eshelonda xakerlar autentifikatsiya va avtorizatsiya jarayonlariga hujumlardan foydalanadilar, sertifikatlashtirish organlariga ishonchni pasaytiradilar, foydalanuvchi identifikatorini soxtalashtiradilar, taqlid qilish va boshqalar.

Virtual xususiy tarmoqlar texnologiyasi VPN (English Virtual Private Network) bugungi kunda nuqta-to-nuqta, tugun-tarmoq va tarmoq-tarmoq turlarining xavfsiz tarmoq ulanishlarini tashkil qilish uchun eng maqbul vositalardan biri hisoblanadi. Uni tashkil qilishda turli xil protokollar va algoritmlar (PPTP, L2TP / IPsec, OpenVPN va boshqalar) ishtirok etishi mumkin, ularga yondashuvni ma'lum vaqt va hisoblash xarajatlari bilan topish qiyin emas. MS-CHAP2 autentifikatsiyasi vaqtida Point-to-Point Tunneling Protocol (PPTP) shu tarzda buzildi. AES (Kengaytirilgan shifrlash standarti) simmetrik blokli shifrlash algoritmidan foydalangan holda IPsec (IP xavfsizligi) psevdo-tasodifiy raqamlar generatori xatosi bilan buzilgan, bu esa tejamkor vaqt ichida ma'lumotni shifrlash xarajatlarini pasaytirdi. Bundan tashqari, OpenSSL kripto kutubxonasining ilgari tasvirlangan zaifligi GNU General Public License (GNU General Public License) ostida tarqatiladigan OpenVPN buzib kirishiga olib kelishi mumkin.

Uskuna va dasturiy ta’minotda (kalitlar, marshrutizatorlar, shlyuzlar, xavfsizlik devorlari, VPN serverlari va boshqalar) shunga o‘xshash xavfsizlik teshiklari mavjud. Bu, birinchi navbatda, IC - proshivkada dasturlash xatolariga bog‘liq.

Skanerlash, zondlash va shifrni ochish mexanizmlaridan foydalangan holda, tajovuzkor hujum qilingan ob'ektning himoya mahsulotini aniqlashi, shuningdek, ulardan foydalanish to‘g‘risidagi ma'lumotlar bilan ob'ektning zaif tomonlari ro‘yxatini olishi mumkin.

Qayd etish joizki, ko‘rib chiqilayotgan texnologiyalarning zaif tomonlari bo‘yicha ishlarni ochiq nashr etish siyosiy va iqtisodiy omillar tufayli bir qator mamlakatlarda rag‘batlantirilmaydi. Bu, shubhasiz, tadqiqot ishlarining borishini murakkablashtiradi.

Xavfsiz kanallar (jumladan, algoritmlar, protokollar, vositalar va texnologiyalar) orqali harakatni boshqarish usullarini yuqorida ko‘rib chiqishdan shuni ko‘rsatadiki, har qanday bepul yoki tijorat axborot xavfsizligi mahsuloti birinchi navbatda dasturlashtirilgan "qattiq" mantiq bilan belgilanadigan o‘ziga xos zaifliklarga ega.

AKT rivojining asosiy tendentsiyalaridan biri bu overlay tarmoqlarni tadqiq qilish

ISSN (E): 2181-4570 ResearchBib Impact Factor: 6,4 / 2024 SJIF 2024 = 5.073/Volume-3, Issue-1

va rivojlantirishdir (inglizcha Overlay Network dan). Bu atama mavjud global kompyuter tarmog‘i Internet ustida ishlaydigan mantiqiy tarmoqni tashkil qilishni anglatadi. VPN tarmoqlarini tashkil qilish uchun ilgari ko‘rib chiqilgan texnologiyalar va PPTP protokoli (1.2-bandga qarang) "overlay" atamasi bilan bog‘liq bo‘lishi mumkin. Ushbu mavzu doirasidagi tadqiqot ishlari quyidagi maqsadlarga asoslanadi:

1) TCP/IP stekining yangi protokollarini, shu jumladan tizimning mavjud arxitekturasiga mos kelmaydigan protokollarini tadqiq qilish, ishlab chiqish va sinovdan o‘tkazish uchun real muhitni tashkil etish (xususan, IPv6 protokoli xususiyatlarini o‘rganish);

2) taqsimlangan hisoblash va axborotni markazlashmagan saqlashni ishlab chiqish va tadqiq qilish;

3) tarmoq xususiyatlarini kengaytirish: maqsadli IP-manzilni ko‘rsatmasdan marshrutlashdan protokollarning kriptoga chidamliligini oshirishgacha;

4) global Internetda anonimlikni ta'minlash.

Afsuski, asosiy urg‘u oxirgi nuqtaga qaratilgan (anonim/anonim tarmoqlar), bu turli mamlakatlar hukumatlarini foydalanish uchun ba'zi texnologiyalarni "tavsiya qilmaslikka" majbur qiladi.

Overlay tarmoqlarini yaratish masalasida, aloqa kanalining o‘tkazish qobiliyati va tezligini optimallashtirish, anonimlik darajasi, axborot xavfsizligi va foydalanish qulayligi o‘rtasida murosani ta'minlashi kerak bo‘lgan trafikni boshqarish usullarini ishlab chiqish ustuvor vazifadir.

Yuqori darajada ixtisoslashgan anonim anonimlashtirilgan tarmoqlar qo‘shimcha tarmoqlarning eng oddiy turi hisoblanadi. Misol sifatida JAP (Java Anonim Proksi) loyihasini ko‘rib chiqing. Uning maqsadi HyperText Transfer Protocol ishini, ya'ni veb-trafikni anonimlashtirishdir va aralash-tugunga asoslangan harakatni boshqarish usuli qo‘llaniladi. Mijoz ma'lumotlarni kerakli adresatga emas, balki turli xil mijozlarning axborot oqimlarini multiplekslashtirgan va ularning haqiqiy adresatlariga so‘rovlar yuboradigan miks serverlar kaskadlari xostiga yuboradi. Javoblar xuddi shu marshrut bo‘ylab uzatiladi. Mijoz-server o‘zaro aloqasi serverlar zanjirini sozlash imkoniyatisiz shifrlangan.

Shunday qilib, oraliq tugunlar kuzatuv ko‘rsatmalarini qayta ishlaydi va jo‘natuvchi va qabul qiluvchining manzilini, shuningdek xabarning mazmunini bilmaydi. Ta'riflangan usulning asosiy kamchiliklari:

ISSN (E): 2181-4570 ResearchBib Impact Factor: 6,4 / 2024 SJIF 2024 = 5.073/Volume-3, Issue-1

1) identifikatsiya qilish (bosh tugunlar va xostlar ro‘yxati hamma uchun ochiq);

2) o‘ziga o‘xshashlik, korrelyatsiya (paketlarni parchalash amalga oshirilgan bo‘lsa-da, tugunlarda trafikni translyatsiya qilishda vaqt kechikishlarida stokastik o‘zgarishlar yo‘q);

3) chiqish tugunida murosaga kelish (ma'lumotlarni asl ko‘rinishida qabul qilish), qo‘shimcha foydalanuvchi shifrlash qatlamini joriy etish zarurati;

1.7-rasm. Piyozga asoslangan transportni boshqarish usuli marshrutlash

Gnutella2 va I2P loyihalarida trafikni boshqarish usullarini tahlil qilgandan so‘ng tahdidlar va hujum turlari mantiqiyroq bo‘ladi. Birinchisi, mantiqiy markazlarni joriy qilish bilan tarmoq qatlami orqali xavfsiz peer-to-peer P2P ulanishini tashkil qilishni o‘z ichiga oladi. Zaif xesh-funksiyalar tarmoq “qurtlari”ning ko‘payishiga olib keladi, qalbakilashtirish va taqlid qilish hujumlari mavjud. Ko‘rinmas Internet loyihasi (I2P) xavfsiz, anonim, o‘z-o‘zini tashkil etuvchi, taqsimlangan, ustki qatlamli tarmoqdir [62]. TCP/IP modelining tepasida ishlaydigan o‘z protokol stekiga ega. Tarmoq ilovalar uchun transport mexanizmini taqdim etadi xabarlarni anonim va xavfsiz yo‘naltirish uchun. O‘zgartirilgan DHT Kademlia xeshlangan tarmoq xost manzillari, AES shifrlangan IP manzillari, ND va umumiy shifrlash kalitlarini saqlash uchun ishlatiladi. Texnologiya barcha ish darajalarida ehtiyotkorlik bilan ko‘rib chiqilishi kerak. Ammo qisqalik uchun faqat kombinatsiyalangan tunnellashtirishga asoslangan I2P trafikni boshqarishning

ISSN (E): 2181-4570 ResearchBib Impact Factor: 6,4 / 2024 SJIF 2024 = 5.073/Volume-3, Issue-1

asosiy kontseptsiyasini eslatib o‘tish kerak (1.9-rasm). Kiruvchi tunnellar tunnel yaratuvchisidan datagrammalarni jo‘natish uchun mo‘ljallangan, chiquvchi tunnellar esa tunnel yaratuvchisiga datagrammalarni yetkazib berish uchun javobgardir.

Xulosa qilib aytishimiz mukinki Ethernet kartasiga integratsilanuvchi apparat majmuasining arxitekturasini ishlab chiqish va tarmoq trafigini shifrlashni ta'minlashga bag'ishlangan. Muammo, TCP/IP protokoli asosida paketli kommutatsiyalangan kompyuter tarmoqlarida (Ethernet) ma'lumotlarni xavfsiz uzatish zaruriyatidan kelib chiqadi. O'zbekistondagi Mudofaa Vazirligi Axborot-kommunikatsiya texnologiyalari va aloqa harbiy instituti tomonidan amalga oshirilayotgan tadqiqotlar shuni ko'rsatadiki, internet orqali ma'lumotlarga bo'lgan talab ortib borishi bilan, xavfsizlik masalalari ham dolzarb bo'lmoqda. TCP/IP protokollari asosidagi korporativ tarmoqlar, xususan, axborotni o'g'irlash va buzish xavfini tug'diradi. Shu sababli, kriptografik himoyalanishga bo'lgan talab ham kuchaymoqda. Maqolada shuningdek, Ethernet kartasida shifrlovchi apparat majmuasini ishlab chiqish, ma'lumotlarni autentifikatsiyalash, kriptografik himoya va ma'lumotlarning yaxlitligini ta'minlash kabi vazifalar ko'rsatilgan. Axborot-kommunikatsiya texnologiyalari davlatlararo raqobatbardoshlik va milliy xavfsizlikka muhim ta'sir ko'rsatadi. Shuningdek, korporativ kompyuter tarmoqlarida trafikni boshqarish va axborot xavfsizligi masalalari, shuningdek, mavjud tizimlar va standartlarning zaifliklari ham tahlil qilinadi. Ushbu maqola, kompyuter tarmoqlarining xavfsizligini, shuningdek, ma'lumotlar uzatish jarayonini optimallashtirish va himoya qilishda zamonaviy yondashuvlarni tadqiq qiladi. Maqola yakunida, xavfsiz kanallar orqali ma'lumotlar uzatishni ta'minlash va yangi protokollarni ishlab chiqish zarurligi ta'kidlangan. Anonim va xavfsiz tarmoqlarni yaratish bo'yicha tadqiqotlar davom ettirilishi, shuningdek, axborot xavfsizligini ta'minlash uchun yangi innovatsiyalarni rivojlantirish kerak. Ushbu tahlil va tadqiqotlar O‘zbekiston Respublikasi uchun axborot kommunikatsiya texnologiyalarining rivojlanishi va samarali qo'llanilishini ta'minlashda muhim ahamiyatga ega.

FOYDALANILGAN ADABIYOTLAR RO‘YHATI

1. Vishnevskiy, VM Markazlashtirilmagan boshqaruv bilan simsiz tarmoqlarni modellashtirish [Matn] / VM Vishnevskiy, AI Lyaxov, BN Tereshchenko // Avtomatlashtirish va telemexanika. - 1999. - No 6. - B. 88–99.

ISSN (E): 2181-4570 ResearchBib Impact Factor: 6,4 / 2024 SJIF 2024 = 5.073/Volume-3, Issue-1

2. Verbitskiy, S. N. Xizmat ko‘rsatish stavkasini boshqarishning optimal siyosatini raqamli o‘rganish [Matn] / S. N. Verbitskiy, V. V. Rikov // Avtomatlashtirish va telemexanika. - 1998. - No 11. - B. 59–70.

3. Ivnitskiy, V. A. O‘tish ehtimoli uning holatiga bog‘liq bo‘lgan yulduz shaklidagi yopiq navbat tarmog‘i holatining statsionar ehtimolliklari to‘g‘risida [Matn] / V. A. Ivnitskiy // Avtomatlashtirish va kompyuter texnologiyalari. - 1994. - No 6. - B. 29–37.

4. Bakanov, AC Markazlashtirilgan boshqaruvga ega simsiz tarmoqlarning ishlash ko‘rsatkichlarini baholash usuli [Matn] / AC Bakanov, V. M. Vishnevskiy, A. I. Lyaxov // Avtomatlashtirish va telemexanika. - 2000. - No 4. - B. 97-105.

5. Gibbens, RJ Ko‘p parentli tarmoqlarda dinamik marshrutlash [Matn] / R. Gibbens, FP Kelly, SRE Turner // IEEE / Networking bo‘yicha ACM tranzaksiyalari. - 1993. - jild. 1, iss. 2. - B. 261–270.

6. Korilis, YA Stackelberg marshrutlash strategiyalari yordamida tarmoq optimalligiga erishish [Matn] / YA Korilis, AA Lazar, A. Orda // Networking bo‘yicha IEEE / ACM tranzaktsiyalari. – 1997.

7. H. Zaynidinov, O. Mallayev, Parallel algorithm for calculating the learning processes of an artificial neural network. AIP Conference Proceedings 2647, 050006 (2022). doi: https://doi.org/10.1063/5.0104178.

8. Yusupov I, Nurmurodov J, Ibragimov S, Gofurjonov M, Qobilov S. “Calculation of Spectral Coefficients of Signals on the Basis of Haar by the Method of Machine Learning”, 14th International Conference, IHCI 2022, Tashkent, Uzbekistan, October 20–22, 2022, pp 547–558. https://link.springer.com/conference/ihci.

9. Bottou, L. (2010). Large-scale machine learning with stochastic gradient descent. In Proceedings of COMPSTAT'2010, Springer.

10. Kingma, D. P., & Ba, J. (2014). Adam: A method for stochastic optimization. arXiv preprint arXiv:1412.6980.

11. Ruder, S. (2016). An overview of gradient descent optimization algorithms. arXiv preprint arXiv:1609.04747.

12. Goodfellow, I., Bengio, Y., & Courville, A. (2016). Deep learning. MIT press.

13. Hastie, T., Tibshirani, R., & Friedman, J. (2009). The elements of statistical learning: Data mining, inference, and prediction. Springer.

ISSN (E): 2181-4570 ResearchBib Impact Factor: 6,4 / 2024 SJIF 2024 = 5.073/Volume-3, Issue-1

14. Shukla, P. (2019). The Gradient Descent Algorithm and Its Variants. arXiv preprint arXiv:1908.10448. doi: 10.1093/ptep/ptaa104.

15. https://www.baeldung.com/cs/gradient-stochastic-and-mini-batch.