15- LABORATORIYA ISHI

MAVZU: NGN XIZMATLARINI TAQDIM ETISHDA QO'LLANILADIGAN AXBOROT XAVFSIZLIKLARI

1.1 Ishdan maqsad

Keyingi avlod tarmoqlarida xavfsiz aloqa va VoIP tahdidlari o'rganish.

1.2 Laboratoriya mashg'ulotiga topshiriq

Laboratoriya mashg'uloti bo'yicha talabalarga mavzu yuzasidan nazariy bilimlarni egallash talab etiladi. Talaba laboratoriya mashg'uloti uchun shaxsiy topshiriq oladi. Bu topshiriq bo'yicha talaba keyingi avlod konvergent tarmoqlari bo'yicha tushunchalar, Keyingi avlod tarmoqlarida xavfsiz aloqa va VoIP tahdidlari o'rganish bo'yicha nazorat savollariga javob yozib uni o'quv mashg'ulotida himoya qiladi va HEMIS tizimiga yuklaydi.

1.3 Adabiyotlar ro'yxati

1. IMS: IP multimedia subsystem concepts and services, Miika Poiselka & George Mayer, 2009 Publishing by John Wiley&Sons Inc., Hoboken New Jersey, USA.
2. IP multimedia subsystem, Taylor & Francis group, Syed A.Ahson, Muhammad Ilyas. 2009, UK.
3. Optical fiber communication: System and impairments., 2002y., Elseiver scinece, USA

15.4 Nazorat savollari

1. VoIP xizmatlari nimalar kiradi?
2. VoIP tahdilar tasnifi nimalardan iborat?
3. Mavjudlikka qarshi tahdidlar nima?
4. Maxfiylikka qarshi tahdidlar nima?
5. Yaxlitlikka qarshi tahdidlar nima?
6. Ijtimoiy kontekstga qarshi tahdidlar nima?

15.5. Nazariy ma'lumotlar

VoIP xizmatlari telekommunikatsiya sohasi uchun keyingi avlod tarmog'ining (NGN) asosiy muammolaridan biridir. Ushbu texnologiya o'xshash rivojlanayotgan texnologiyalar kabi ijobiy va salbiy tomonlardan iborat. Hozirgi kunda aloqa operatorlari qo'ng'iroqlarni kutish, konferentsiya qo'ng'iroqlari, qo'ng'iroqlarni o'tkazish, qo'ng'iroq qiluvchini identifikatori va boshqa VoIP xizmatlarini NGN va barcha IP yechimlari asosida taqdim etadi. Shunday qilib, VoIP xavfsizligi hozirda ko'plab munozaralar olib boriladigan masalalardan biridir. Ushbu maqolada biz NGN-dagi VoIP xizmatlarining zaiflik toifalariga

e'tibor qaratishga qaror qildik. Biz umumiy xavfsizlik tahdidlari va VoIP xizmatlarining zaif tomonlarini taqdim etishga harakat qilamiz. Zaifliklar va ularning tasnifini aniqlash, shuningdek, ushbu tizim tahdid soladigan xavflar ushbu tizimga kirish yo'llarini aniqlaydi va ma'murlarga muammolarni hal qilish imkonini beradi.

Bu masala bo'yicha bahs-munozaralar turli xil xususiyatlarni to'liq tan olmagan holda noto'g'ri bo'ladi. Bundan tashqari, ushbu turdagi zaifliklarni aniqlash muhimligini aniqlashtirish uchun biz VoIP uchun ehtimoliy tahdidlarni tasniflaymiz.

Hozirgi kunda telekommunikatsiya tarmoqlari hayotimizning ajralmas qismiga aylanib, axborot va yangiliklar almashishda katta rol o‘ynamoqda. 100 yildan ortiq vaqtdan beri mavjud bo'lgan ushbu texnologiya o'zini moslashtirish va yangi avlodlarning yangi talablariga javob berish uchun ilg'or choralarni ko'rdi. IP Multimedia quyi tizimi (IMS) 3GPP (Uchinchi avlod hamkorlik loyihasi) tomonidan ishlab chiqilgan va ishlab chiqilgan Internet protokoli (IP) asosida real vaqt rejimida multimedia xizmatlarini taqdim etadi.

IMSning asosiy maqsadi uyali aloqa tarmoqlari va Internetni birlashtirishdir. Ushbu ikki tamoyilning yaqinlashishi provayderlarga o'z mijozlariga deyarli qayerda bo'lmasin, Internet xizmatlaridan foydalanishni taklif qilish imkonini beradi. IMS bir nechta funktsiyalardan iborat bo'lgan taqsimlangan tizimdir. Ushbu funktsiyalar o'rtasidagi aloqa IP tarmog'iga asoslangan bo'lib, u ba'zi afzalliklarga ega, ammo xavfsizlik muammolari kabi kamchiliklarga ham ega. IMS boshqa texnologiyalar bilan solishtirganda juda ko'p afzalliklarga ega. U ochiq standartga mos keladi va real vaqtda va xizmatga yo'naltirilgan arxitekturaga ega. U o'zining asosiy maqsadi, ya'ni mijozlarga xizmat ko'rsatishni hisobga olgan holda ishlab chiqilgan. U ushbu muhim texnologiyalarni birlashtiradi: mobillik, Internetga tezkor kirish, real vaqt rejimida multimedia xizmatlari, tarmoqni oson boshqarish, yangi xizmatlarni qulay joylashtirish, tarmoqqa mustaqil kirish (u statsionar, kabel va mobil kirish texnologiyalarini qo'llab-quvvatlaydi, shu jumladan WCDMA, CDMA2000, GPRS, Wi-Fi, GSM, 3G), IP muhitida xizmat ko'rsatish sifati, foydalanuvchi va ma'lumotlar xavfsizligi, zaryadlash imkoniyatlari, roumingni qo'llab-quvvatlash va statsionar va mobil tarmoqlarni bir birlikka yaqinlashtirish imkonini beradi.

VoIP tahdilar tasnifi

Ushbu ishda biz VoIP tahdidlarini 4 toifaga ajratdik:

1) Mavjudlikka qarshi tahdidlar
2) Maxfiylikka qarshi tahdidlar
3) Yaxlitlikka qarshi tahdidlar
4) Ijtimoiy kontekstga qarshi tahdidlar

Ushbu toifalarning har biri biz quyida aytib o'tadigan ba'zi tahdidlarni o'z ichiga oladi.

A. Mavjudlikka qarshi tahdidlar

Xatarlarning ayrim guruhlari kuniga 24 soat va haftada 7 kun taqdim

etiladigan xizmatlarga qarshi yaratiladi va tizimning ishlamay qolishi yoki uzilishi va uzilishiga olib keladi. Mashhur misol DoS (Xizmatni rad etish) hujumidir. Ushbu xavflar orasida biz quyidagi misolni ko'rsatishimiz mumkin:

1) Qo'ng'iroq toshqini (ortib ketishi)

DoS-dan mashhur misol - bu bir vaqtning o'zida qo'ng'iroqlarni to'ldirishni yaratish, bunda tajovuzkor haqiqiy yoki noto'g'ri qo'ng'iroqlardan (signal yoki media) og'ir trafikni keltirib chiqaradi va maqsadli tizimga (masalan, VoIP-server, mijoz va asosiy infratuzilma) yuboradi va shu bilan sezilarli darajada uning samaradorligi pasaysa yoki tizim buziladi. Umumiy usullar quyidagilar:

- Yaroqli yoki noto'g'ri ro'yxatdan o'tish
- Yaroqli yoki noto'g'ri so'rov
- Qo'ng'iroqni sozlashdan so'ng qo'ng'iroqlarni nazorat qilish
- Ping ortishi

Nafaqat qasddan qo’ng’iriq toshqini, balki tasodifiy qo’ng’iriq toshqini ham "o'z-o'zidan hujum" deb ataladigan tizimning ishdan chiqishiga olib kelishi mumkin. Quyidagi omillar hujumga sabab bo'lishi mumkin:

Mintaqaviy elektr energiyasini uzish va tiklash

- Qurilmaning noto'g'ri konfiguratsiyasi
- Oxirgi nuqtalarning noto'g'ri ishlashi
- Qonuniy chaqiruv toshqin

2) Noto'g'ri tuzilgan xabarlar (protokol o'chirilishi)

Buzg'unchi noto'g'ri tuzilgan xabarni yaratishi va ishni buzish niyatida uni ma'lum bir foydalanuvchiga yuborishi mumkin. Bu noto'g'ri shakllangan xabar protokol xabariga o'xshaydi, lekin matn noto'g'ri yozilgan va u tegishli qurilmalarda chalkashlikka olib keladi. Ushbu tahdid odatda quyidagi sabablarga ko'ra yuzaga keladi:

- Protokol spetsifikatsiyasining zaifligi
- Noto'g'ri shakllangan xabarni yaratish qulayligi
- Amalga oshirishda istisnolardan foydalanishning yo'qligi
- Barcha noto'g'ri shakllangan holatlarni sinab ko'rish qiyinligi

3) Soxta xabarlar

Buzg'unchi xizmatlarni to'xtatish yoki seansni o'g'irlash uchun soxta (soxta) xabarni kiritishi mumkin. Odatiy misollar "qo'ng'iroqni buzish" va "pullik firibgarlik".

a) Qo'ng'iroqni buzish

Bu usulda tajovuzkor SIP dialog oynasini kuzatib boradi va seans ma'lumotlarini va "Kimdan" va "Kimga" teglarini oladi va aloqa qurilmasiga "SIP BYE" xabarini yuboradi va ongsiz ravishda qo'ng'iroq seansining yopilishiga olib keladi.

4) Qo'ng'iroqlarni o'g'irlash

Qo'ng'iroqlarni o'g'irlash VoIP so'nggi nuqtasi va tarmoq o'rtasidagi ba'zi bir tranzaksiya tajovuzkor tomonidan qabul qilinganda sodir bo'ladi. Odatda ro'yxatga olish, serverni o'g'irlash va media serverni o'g'irlashdir [7].

Bunday holda, tajovuzkor o'zini qonuniy qurilma sifatida tan oladi va ikkita oxirgi nuqta orasidagi barcha aloqa va media seanslarini o'g'irlaydi. Yuboruvchi foydalanuvchi, u kerakli foydalanuvchi bilan suhbatda, deb o'ylaydi, mo'ljallangan foydalanuvchi esa xabar jo'natuvchiga kirish huquqiga ega emas.

5) QoSni suiste'mol qilish

Ushbu usulda tajovuzkor turli xil vositalardan foydalangan holda katta tarmoqli kengligini egallaydi va qonuniy foydalanuvchi xizmatlardan foydalana olmaydi yoki xizmat sifati muammolarga duch keladi.

B. Maxfiylikka qarshi tahdidlar

Oldingi bo'limdagi xizmatning uzilishidan farqli o'laroq, maxfiylikka qarshi tahdidlar umuman joriy aloqalarga ta'sir qilmaydi, lekin ommaviy axborot vositalarini o'g'irlash va yozib olish orqali tajovuzkor keyingi tahdid uchun zarur bo'lgan ma'lumotlarni oladi. Bu maxfiylikka tahdidlarning eng mashhur turlarini taqdim etadi.

1) OAVlarni tinglash

Axborot vositalarini tinglash ikki usulda amalga oshiriladi. Ulardan biri maqsadli foydalanuvchi bilan bir xil eshittirish domenidagi media paketlarni hidlashdir. Ikkinchisi kirish moslamasini buzish (masalan, qatlam 2 kaliti) va tajovuzkor qurilmaga yo'naltirish va ko'paytirishdir [7].

2) Chaqiruv namunasi yuk tashish

Ushbu usulda tajovuzkor VoIP xizmatini ruxsatsiz tahlil qilishda davom etadi va kerakli ma'lumotlarni oladi. Misol uchun, kompaniyaning bosh direktori va moliyaviy direktori boshqa kompaniyaning bosh direktori va moliya direktoriga qo'ng'iroq qilganini bilish, sotib olish davom etayotganini ko'rsatishi mumkin.

3) Trafikni ushlab turish

Traffic Capture bu trafikni har qanday vosita bilan ruxsatsiz yozib olish bo'lib, paketlarni yozib olish va ruxsatsiz maqsadlarda paketlarni kuzatishni o'z ichiga oladi. Trafikni yozib olish barcha tomonlarning roziligisiz muloqotni yozib olishning asosiy usuli hisoblanadi.

4) Ma'lumotlarni qidirish

Foydalanuvchi nomi, telefon raqami, URL manzili, elektron pochta manzili yoki tajovuzkor quyidagi sabablarga ko'ra foydalanadigan boshqa identifikatorlar kabi ma'lumotlarni to'plang: pullik firibgarlik qo'ng'iroqlari, spam qo'ng'iroqlar, xizmatdagi uzilishlar, fishing.

5) Xizmatni suiste'mol qilish

Xizmatdan suiste’mol qilish xizmatlardan noto'g'ri foydalanishning katta toifasi bo'lib, quyidagilarni o'z ichiga oladi:

a) Konferentsiyani suiste’mol qilish

Conference Conference suiste’moli - bu firibgarlik qilish maqsadida shaxsni yashirish vositasi sifatida VoIP qo'ng'iroq xizmatidan suiste’mol qilish.

b) Premium tarif xizmati (PRS) firibgarligi

Premium tarif xizmati firibgarligi - bu hisob-kitoblarni maksimal darajada

oshirishdan tashqari, roziliksiz yoki maqsadsiz trafikni sun'iy ravishda oshirish usuli.

c) noto'g'ri chetlab o'tish yoki hisob-kitobni sozlash

Noto'g'ri aylanib o'tish yoki to'lovga tuzatishlar - bu vakolatli xizmat to'lovlaridan qochish yoki hisob-kitob yozuvlarini o'zgartirish orqali boshqa firibgarliklarni yashirish usullari.

C. Yaxlitlikka qarshi tahdidlar

Buzg'unchi xabarni tarmoq interfeysi sifatida ushlab olgandan so'ng, u o'zgartirishga harakat qiladi. O'zgartirish VoIP xabari yoki mediadagi ma'lum ma'lumotlarni o'chirish, kiritish yoki almashtirishdan iborat bo'lishi mumkin.

Ushbu bo'lim ikki turga bo'linadi:

- Xabar yaxlitligiga qarshi tahdidlar (xabarni o'zgartirish)
- OAV yaxlitligiga qarshi tahdidlar (ommaviy axborot vositalarini o'zgartirish)

Xabarning yaxlitligiga tahdid (xabarni o'zgartirish) quyidagi usullar bilan amalga oshiriladi:

1) Call Rerouting Qo'ng'iroqlarni yo'naltirish

Qo'ng'iroq marshrutlash ma'lumotlariga ruxsatsiz kirish tajovuzkorning kirishi qo'ng'iroq yo'nalishini o'zgartiradi va kerakli foydalanuvchiga murojaat qilish o'rniga qo'ng'iroq boshqa joyga o'tkaziladi.

2) Call black holing Qora ruyxatni chaqiring

Protokol xabarining har qanday muhim elementlarini o'chirish yoki uzatishni rad etishning ruxsat etilmagan har qanday usuli. Buning oqibati qo'ng'iroqni sozlashni kechiktirish, keyingi xabarlarni rad etish, dasturda xatolarga yo'l qo'yish, qo'ng'iroq ulanishlarini uzish va hokazo.

3) Soxta qo'ng'iroq qiluvchining identifikatsiyasi

Noto'g'ri qo'ng'iroq qiluvchini identifikatsiya qilish - bu noto'g'ri shaxs yoki mavjudligi haqida signaldir.

Ommaviy axborot vositalarining yaxlitligiga qarshi tahdidlar (ommaviy axborot vositalarini o'zgartirish) quyidagi usullar bilan amalga oshiriladi:

a) media in'ektsiya

Ushbu usulda tajovuzkor yangi mediani faol media kanaliga kiritadi yoki faol media kanalidagi mediani almashtiradi. Natijada foydalanuvchi (jabrlanuvchi) suhbat o'rtasida reklama, shovqin yoki jimlikni eshitishi mumkin.

b) ommaviy axborot vositalarining degradatsiyasi

Buzg'unchi media boshqaruv paketlarini manipulyatsiya qiladi va har qanday aloqaning QoS darajasini pasaytirishga olib keladi.

D. Ijtimoiy kontekstga qarshi tahdidlar

Bu tahdid boshqa tahdidlardan biroz farq qiladi. Ushbu usulda tajovuzkor o'zini ishonchli shaxs sifatida noto'g'ri ko'rsatadi va shaxsiy ma'lumotlarni olish va navbatdagi tahdidni amalga oshirish uchun maqsadli foydalanuvchiga (jabrlanuvchiga) yolg'on ma'lumot beradi.

Ijtimoiy kontekstga qarshi tipik tahdidlar quyidagilar:

- Shaxs, vakolat, huquq va mazmunni noto'g'ri ko'rsatish
- Qo'ng'iroq (ovoz), IM va mavjudligi spami

Fishing

1) shaxs, vakolat, huquq va mazmunni noto'g'ri ko'rsatish

Soxta identifikatorni taqdim etish orqali foydalanuvchi (jabrlanuvchi) aldanishi mumkin va tajovuzkor parol, kalit, sertifikat va hokazolarga kirish huquqiga ega bo'ladi.

2) Qo'ng'iroq spami (ovoz), IM va mavjudligi

Internet-marketingda eng koʻp qoʻllaniladigan audio yoki video seans yaratish boʻyicha nomaqbul soʻrovlarning katta miqdori.[9] Ushbu bo'lim uch turga bo'linadi:

Qo'ng'iroqlar spami (SPIT - Call Spam)

- Tezkor xabarlar orqali spam yoki IM spam (SPIM - pam over Instant Messaging or IM Spam)
- Spam mavjudligi (SPPP - Presence spam)