SIMSIZ TARMOQLARDA XAVFSIZLIK MUAMMOLARI

Ibragimov Sh.M.[1], Umarov B.A.[2] , Abdusattorova M.V.[3]
[1]Farg'ona davlat universiteti Axborot texnologiyalari kafedrasi dotsenti, shavkat19702008@gmail.com
[2]Farg'ona davlat universiteti o'quv ishlari bo'yicha dekan o'rinbosari, ubaumarov@gmail.com
[3]Farg'ona davlatunversiteti3-kurs talabasi, mohigulabdusattorova50@gmail.com

Annotasiya. *Simsiz tarmoqlarning xavfsizlik muammolarini, jumladan ruxsatsiz kirish, ma'lumotlarni ushlash va Wi-Fi tarmoqlaridagi zaifliklarni tahlil qiladi. Shuningdek, mobil tarmoqlarda keng tarqalgan tahdidlar, masalan "o'rtadagi odam" hujumlari va shifrlashdagi kamchiliklar ko'rib chiqiladi. Maqolada ushbu muammolarni bartaraf etish bo'yicha asosiy tavsiyalar beriladi.*

Kalit so'zlar. *Simli tarmoqlar xavfsizligi, ruxsatsiz kirish, Wi-Fi zaifliklari, ma'lumotlarni shifrlash, hujum modellari, mobil tarmoq tahdidlari.*

KIRISH. Bugungi kunda simsiz tarmoqlar (Wi-Fi, mobilaloqa, Bluetooth, Zigbeeva boshqalar) kundalik hayotimizning ajralmas qismiga aylangan. Uylar, ofislar, jamoat transportlari, kafelar, aeroportlar, deyarli hamma joyda internetga simsiz ulanish imkoniyati mavjud. Biroq, qulaylik bilan birga xavfsizlik masalalari ham kun tartibidagi eng dolzarb muammolardan biriga aylandi. Simsiz muhitdagi ma'lumotlar efir orqali tarqalgani sababli, ularni tutib olish, o'zgartirish yoki blokirovka qilish simli tarmoqlarga nisbatan ancha oson. Ushbu maqolada simsiz tarmoqlarning asosiy xavfsizlik muammolari, ushbu muammolardan kelib chiqadigan xatarlar va ularga qarshi qo'llaniladigan himoya choralari atroflicha tahlil qilinadi.

Simsiz tarmoqlarda ma'lumotlar elektromagnit to'lqinlar yordamida uzatiladi. Bunda fizik muhit (kabel) mavjud emas. Har qanday qabul qilgich, agar to'g'ri chastotada sozlangan bo'lsa, uzatilayotgan paketlarni "eshitishi" mumkin. Bu holat simli tarmoqlarda uchramaydi, chunki simli tarmoqqa jismoniy kirish talab qilinadi. Shu sababli simsiz tarmoqlar tabiatan "ochiq" muhit hisoblanadi.

Xavfsizlikning uch asosiy komponenti quyidagilar: maxfiylik (confidentiality), butunlik (integrity) va mavjudlik (availability) simsiz tarmoqlarda zaif hisoblanadi. Masalan, oddiy himoyalanmagan Wi-Fi tarmog'ida hech qanday maxfiy kalitsiz ma'lumotlarni o'qish mumkin. Bu esa shaxsiy ma'lumotlarning oshkor bo'lishi, firibgarlik va boshqa jinoyatlar uchun zamin yaratadi.

Ko‘plab foydalanuvchilar routerlarini zavod sozlamalarida qoldiradi. Standart administrator login-parollar (admin/admin, root/1234) tajovuzkorlar uchun birinchi “eshik”dir. Shuningdek, WPS funksiyasi orqali ham qisqa vaqt ichida parolni tanlab olish mumkin. Ruxsatsiz kirish natijasida tajovuzkor nafaqat internetdan tekin foydalanadi, balki tarmoqdagi qurilmalarga hujum uyushtirishi, ularni botnet tarkibiga qo‘shishi yoki muhim fayllarni o‘g‘irlashi mumkin.

Simsiz muhitda eng keng tarqalgan tahdid bu “passiv tinglash”dir. Tajovuzkor maxsus dasturiy vositalar (masalan, Wireshark, Aircrack-ng) yordamida tarmoqdagi barcha trafikni ushlay oladi. Agar ma’lumotlar shifrlanmagan bo‘lsa (masalan, HTTP saytlar, oddiy pochta protokollari), login, parol, bank kartasi ma’lumotlari bemalol o‘qiladi. Hatto WEP shifrlashni bir necha daqiqada buzib kirishi mumkin.

Bu hujumda tajovukor ikki qonuniy foydalanuvchi o‘rtasidagi aloqaga aralashadi. Masalan, soxta Wi-Fi nuqtasi (Evil Twin) yaratilib, foydalanuvchi uni haqiqiy router deb biladi. Barcha ma’lumotlar tajovuzkor orqali o‘tadi, u ularni o‘zgartirishi yoki o‘qishi mumkin. MITM hujumi ayniqsa jamoat Wi-Fi tarmoqlarida keng tarqalgan.

Ofis yoki uy tarmog‘iga xodim yoki tashrifchi tomonidan o‘zining shaxsiy routeri ulansa, bu “rogue AP” deb ataladi. Bunday nuqtalar ko‘pincha xavfsizlik siyosatiga zid ravishda o‘rnatiladi va korporativ tarmoqqa kirish eshigiga aylanadi. Tajovuzkor bu nuqta orqali tarmoqqa kirib, ma’lumotlarni o‘g‘irlashi mumkin.

WEP (Wired Equivalent Privacy) 1997-yilda ishlab chiqilgan, ammo hozirda butunlay xavfsiz emas. RC4 shifridagi statistik zaifliklar tufayli bir necha daqiqada parchalanadi.

WPA2 hozirgacha eng keng tarqalgan. Biroq 2017-yilda KRACK (Key Reinstallation Attack) hujumi topilgan. Bu hujum WPA2 ning 4-tomonlama qo‘l siqish jaroyonidagi kamchilikdan foydalanadi.

Yangi protokol, ammo hali hamma qurilmalar tomonidan qo‘llab-quvvatlanmaydi. Dastlabki tadqiqotlar WPA3 da ham ba’zi zaifliklar borligini ko‘rsatgan (masalan, Dragonblood zaifliklari).

Simsiz tarmoqlarda “mavjudlik”ka qarshi hujumlar oson. Deauthentication hujumida tajovuzkor soxta boshqaruv paketlarini yuborib, foydalanuvchini routerdan uzib qo‘yadi. Bu esa xizmat ko‘rsatishni to‘xtatish (DoS) holatiga olib keladi. Jamoat Wi-Fi tarmoqlarida bunday hujumlar xizmatdan foydalanishni imkonsiz qiladi.

Mobil aloqa tarmoqlari (LTE, 5G) simsiz Wi-Fi tarmoqlariga qaraganda ancha murakkab va nazariy jihatdan xavfsizroq hisoblanadi. Biroq ularning ham zaif tomonlari bor.Imsi-catcher (yoki “Stingray”) qurilmalari soxta baza stantsiyasi vazifasini bajarib, abonentlarning IMSI identifikatorlarini yig‘adi va suhbatlarni tinglaydi. 5G da signaling zaifliklari hali to‘liq bartaraf etilmagan. SS7 protokolidagi kamchiliklar tufayli xalqaro roumingda foydalanuvchi joylashuvini aniqlash va SMS xabarlarni o‘qish mumkin.

Mobil ilovalardagi xavflar: ko‘plab ilovalar ruxsatsiz holda Wi-Fi va mobil ulanish holatiga kirib, foydalanuvchi ma’lumotlarini uchinchi tomonlarga yuboradi.

WPA3 protokoliga o‘tish (agar qurilmalar qo‘llab-quvvatlasa). Aks holda WPA2-AES (TKIP emas) sozlamalari. Uzun va murakkab parollar (kamida 12 belgi, harflar, raqamlar, belgilar). Enterprise usulida (802.1X) autentifikatsiya – har bir foydalanuvchi uchun alohida login-parol yoki sertifikat. MAC-filtrlash (to‘liq himoya qilmasa-da, qo‘shimcha qatlam). Rogue AP deteksiyasi uchun maxsus dasturiy vositalar (masalan, WIDS - Wireless Intrusion Detection System). Router proshivkasini muntazam yangilab turish.

Agar uy yoki ofisda bir nechta qurilma bo‘lsa (masalan, smart TV, IoT sensorlari, kompyuterlar), ularni turli VLAN yoki “guest network” orqali ajratish maqsadga muvofiq. Bitta qurilma buzilgan taqdirda ham boshqalar xavfsiz qoladi.

Jamoat Wi-Fi tarmoqlarida VPN (Virtual Private Network) ishlatish. VPN barcha trafikni shifrlaydi va MITM hujumidan himoya qiladi. HTTPS saytlardan foydalanish (qavariqda yashil qulf belgisi). Telefon va kompyuterlarda o‘rnatilgan antivirus va xavfsizlik dasturlari. Simsiz tarmoqdan foydalanmayotganda routerning qo‘shimcha xizmatlarini (WPS, Telnet, UPNP) o‘chirish.

Xulosa. Simsiz tarmoqlar hayotimizni qulaylashtirgan bo‘lsa-da, ularning ochiq muhiti jiddiy xavfsizlik xatarlarini keltirib chiqaradi. Ruxsatsiz kirish, ma’lumotlarni tinglash, MITM hujumlari, zaif shifrlash protokollari va DoS hujumlari eng keng tarqalgan tahdidlardir. Ushbu muammolarni hal qilish uchun texnik choralar (WPA3, VPN, monitoring) bilan birga foydalanuvchilarning xabardorligini oshirish va doimiy xavfsizlik siyosatiga rioya qilish zarur.

Zero Trust tamoyili, muntazam yangilanishlar va kuchli parollar simsiz muhitda ma’lumotlar xavfsizligining asosiy kafolatidir. Har bir foydalanuvchi o‘zining uy routeridan tortib, jamoat Wi-Fi tarmog‘igacha ehtiyotkor bo‘lishi kerak. Kelajakda sun’iy intellekt va kvant kriptografiyasi simsiz tarmoqlar xavfsizligini yangi bosqichga olib chiqadi, ammo hozircha eng ishonchli himoya bu o‘z bilim va odatlarimizdir.

Adabiyotlar ro’yhati

1. Karimov A. R. – Kompyuter tarmoqlari va ularning xavfsizligi. Toshkent: “Fan va texnologiya” nashriyoti, 2020. – 245 b. (3-bob: Simsiz tarmoqlar va himoya mexanizmlari)

2. Rahmatullayev Sh. M., Tojiboyeva D. K. – Axborot xavfsizligi asoslari. Toshkent: “Moliya” nashriyoti, 2019. – 312 b. (5-bob: Wi-Fi va mobil aloqa xavfsizligi)

3. Olimov B. T. – Kriptografiya va tarmoqlarda himoya. Toshkent: TATU nashriyoti, 2021. – 198 b. (4-bob: Simsiz protokollardagi kriptografik zaifliklar)

4. Sultonova N. J., Ergashev O. X. – Zamonaviy tarmoq texnologiyalari va xavfsizlik muammolari. Samarqand: SamDU nashriyoti, 2022. – 176 b. (2-bob: IEEE 802.11 standarti va hujumlari)

5. Yusupov B. E. – Axborot tizimlarida xavfsizlik auditi. Toshkent: “Iqtisod-Moliya” nashriyoti, 2018. – 290 b. (6-bob: Simsiz tarmoqlarni zaiflikka tekshirish metodikasi)