TOSHKENT MENEJMENT VA IQTISODIYOT INSTITUTI

MANAGEMENT AND ECONOMICS SCIENTIFIC RESEARCH JOURNAL

2-TO'PLAM
1-MAXSUS SON/2025

MANAGEMENT AND ECONOMICS SCIENTIFIC RESEARCH JOURNAL

MENEJMENT VA IQTISODIYOT ILMIY-TADQIQOT JURNALI

НАУЧНО-ИССЛЕДОВАТЕЛЬСКИЙ ЖУРНАЛ МЕНЕДЖМЕНТА И ЭКОНОМИКИ

journals@timeedu.uz

+998 95 651 90 00

MANAGEMENT AND ECONOMICS
SCIENTIFIC RESEARCH JOURNAL

+998 95 651 90 00
journals@timeedu.uz
Shota Rustaveli ko'chasi, 114
tmijournals.ndc-agency.uz
@TMII_ilmiy_bolim

Bosh muharrir:
Narbayev Sharafatdin Kengeshovich

Bosh muharrir o‘rinbosari:
Nosirova Nargiza Jamoliddin qizi

Muharrir:
Qarshiyeva Shahnoza Davlatovna

Tahrir hay’ati:

1. Sharipov Kongratbay Avezimbetovich – O‘zbekiston Respublikasi Oliy ta’lim, fan va innovatsiyalar vaziri, t.f.d., prof.;
2. Axmedov Xojiakbarxon Dilshatovich – Toshkent menejment va iqtisodiyot instituti rektori i.f.n., dotsent;
3. Gulyamov Saidasror Saidaxmedovich – O‘zbekiston Fanlar akademiyasi akademigi, i.f.d, professor;
4. Gulyamov Saidaxror Saidaxmedovich – O‘zbekiston Fanlar akademiyasi akademigi i.f.d, professor;
5. Sultanov Mansur Qilichovich – Oliy ta’lim, fan va innovatsiyalar vazirligi huzuridagi “Inno” innovatsion o‘quv-ishlab chiqarish texnoparki bosh direktori, t.f.f.d., dotsent;
6. Chertovitskiy Aleksandr Stepanovich - „Toshkent irrigatsiya va qishloq xo‘jaligini mexanizatsiyalash muxandislari instituti“ Milliy tadqiqot universiteti professori, iqtisodiyot fanlari doktori;
7. Popkova Yelena Gennadyevna - Rossiya Federatsiyasi avtonom notijorat tashkiloti "Ilmiy kommunikatsiyalar instituti" prezidenti, iqtisodiyot fanlari doktori, professor;
8. Dr Goh Khang Wen – Malaziyaning INTI Xalqaro universiteti prorektori;
9. Wang Cheng – XXR “Hebei Institute of Mechanical and Electrical Technology” instituti i.f.f.d., dotsent;
10. Yo‘ldoshev Nuriddin Qurbonovich – Toshkent menejment va iqtisodiyot instituti Biznes boshqaruvi va moliya kafedrasi i.f.d., professor;
11. Akramov Tohir Abdirahmonovich Toshkent menejment va iqtisodiyot instituti Biznes boshqaruvi va moliya kafedrasi i.f.d., professor;
12. Temirov Abdulaziz Alimjonovich – Toshkent menejment va iqtisodiyot instituti Biznes boshqaruvi va moliya kafedrasi i.f.n, professor;
13. Rajabov Nazirjon Razzaqovich – Toshkent menejment va iqtisodiyot instituti Iqtisodiyot kafedrasi mudiri, i.f.n., dotsent;
14. Xotamov Ibodullo Sadulloyevich – Toshkent menejment va iqtisodiyot instituti Iqtisodiyot kafedrasi i.f.n., professor;
15. Sobirov Aziz Avazbekovich – Toshkent menejment va iqtisodiyot instituti Biznes boshqaruvi va moliya kafedrasi mudiri, i.f.f.d., dotsent;
16. Raximova Shahlo Baxtiyorovna – Ta’lim sifatini nazorat qilish bo‘limi boshlig‘i, p.f.f.d., dotsent;
17. Kadirova Istora Bobirovna – Toshkent menejment va iqtisodiyot instituti Karyera markazi direktori, i.f.f.d.;
18. Turakulov Otabek Xolmirzayevich – Toshkent menejment va iqtisodiyot instituti Muhandislik va axborot texnologiyalari kafedrasi mudiri, t.f.f.d.

MUHANDISLIK OYLIGI

“RAQAMLI TEXNOLOGIYALARNI RIVOJLANTIRISH VA INNOVATSION MUHANDISLIK YECHIMLARI: ZAMONAVIY TENDENSIYALAR VA ISTIQBOLLAR” MAVZUSIDA RESPUBLIKA ILMIY-AMALIY ANJUMANI TO’PLAMI MATERIALLARI

17-18 APREL, 2025
TOSHKENT

MUNDARIJA

4-SHO‘BA: KIBERXAVFSIZLIK VA MA'LUMOTLARNI HIMOYA QILISH

OCHIQ WI-FI TARMOQLAR XAVFSIZLIGI

Haydarov E.D.,
Muhammad Al-Xorazmiy nomidagi
Toshkent axborot texnologiyalari universiteti
Axborot xavfsizligi kafedrasi mudiri, PhD
Dusmurodov Q.A.
Muhammad Al-Xorazmiy nomidagi
Toshkent axborot texnologiyalari universiteti
Kriptologiya kafedrasi magistranti

Annotatsiya. *Ochiq WiFi tarmoqlari keng qo‘llanilayotgan bir paytda, bunday tarmoqlarni himoyalash muhim ahamiyat kasb etadi. Ushbu maqolada ochiq simsiz tarmoqlar va ularning xavfsizligi tahlil etilgan. Yangi Wireless Access Protocol — WPA3 joriy etilishi bilan ochiq tarmoqlarning xavfsizligi sezilarli darajada yaxshilandi. Biroq, evil twin (soxta tarmoq) hujumlariga qarshi kurashishda WPA3 protokolida hech qanday o‘zgarishlar kiritilmagan, shu sababli bu turdagi hujumlar hanuzgacha mumkin bo‘lgan xavf turlaridan biri hisoblanadi. Maqolada WPA3 dagi yangi texnikalar va protokollar tahlil qilingan. Shuningdek, evil twin hujumlariga qarshi foydalanuvchini himoya qilishning bir nechta yondashuvlari taklif etilgan. Tanlangan mezonlar asosida eng yaxshi deb topilgan yondashuv — “birinchi foydalanishda ishonch” (trust on first use) usuli tanlab olinib, uni qanday qo‘llash bo‘yicha tavsiyalar keltirilgan.*
Kalit so’zlar: *Wireless Access Protocol, Wi-Fi, WPA1, WPA2, WPA3, Soxta tarmoq, Password Cracking, Eavesdropping, Evil twin attack, Opportunistic Wireless Encryption, Simultaneous Authentication of Equals.*

Abstract. *With the widespread use of open Wi-Fi networks, ensuring their security is becoming increasingly important. This article analyzes open wireless networks and their security. With the introduction of a new wireless access protocol, WPA3, the security of open networks has increased significantly. However, no changes were made to the WPA3 protocol to combat evil twin attacks, so this type of attack still poses a potential threat. This article analyzes new WPA3 technologies and protocols. Several approaches to protecting the user from evil twin attacks were also proposed. Based on the selected criteria, the best approach, the “trust from first use” method, was selected and recommendations for its use were given.*
Keywords: *Wireless Access Protocol, Wi-Fi, WPA1, WPA2, WPA3, Fake Network, Password Cracking, Eavesdropping, Evil Twin Attack, Opportunistic Wireless Encryption, Simultaneous Peer Authentication.*

Аннотация. *В связи с широким распространением открытых сетей Wi-Fi обеспечение их безопасности становится все более важным. В статье анализируются открытые беспроводные сети и их безопасность. С внедрением нового протокола беспроводного доступа — WPA3 — безопасность открытых сетей значительно повысилась. Однако в протокол WPA3 не было внесено никаких изменений для борьбы с*

атаками типа «злой близнец», поэтому этот тип атак по-прежнему представляет потенциальную угрозу. В статье анализируются новые технологии и протоколы WPA3. Также было предложено несколько подходов к защите пользователя от атак «злых близнецов». На основании выбранных критериев был выбран наилучший подход — метод «доверия с первого использования» — и даны рекомендации по его применению.

Ключевые слова: *Протокол беспроводного доступа, Wi-Fi, WPA1, WPA2, WPA3, поддельная сеть, взлом паролей, подслушивание, атака «злого близнеца», оппортунистическое беспроводное шифрование, одновременная аутентификация равных.*

Kirish

Ommaviy Wi-Fi tarmoqlari tobora ko‘proq qo‘llanilmoqda va bugungi kunda turli joylarda uchrashi mumkin. Mahalliy qahvaxonada bo‘ladimi, yaqin atrofdagi supermarketdami yoki har kuni foydalaniladigan poezddami — aksariyat odamlar vaqti-vaqti bilan bunday ochiq tarmoqlardan foydalanadi. Afsuski, bu tarmoqlar xavfsiz emas. Ushbu ishda shunday tarmoqlardagi xavfsizlikni oshirishga qaratilgan.

Hozirgi kunda aksariyat Wi-Fi tarmoqlari Wireless Protected Access 2 (WPA2) protokolidan foydalanadi, ommaviy tarmoqlarda esa umuman xavfsizlik chorasi ko‘rilmaydi. Bu esa hujumchiga bir nechta turdagi hujumlarni amalga oshirish imkonini beradi. Ochiq tarmoqlarda hujumchi tarmoqqa ulanib, tarmoqda yuborilayotgan barcha ma’lumotlarni yashirincha kuzatishi mumkin, chunki bu holatda hech qanday shifrlash qo‘llanilmaydi. Agar tarmoq WPA2 orqali himoyalangan bo‘lsa ham, agar hujumchi tarmoq ichida bo‘lsa, barcha ma’lumotlarni kuzatishi mumkin, chunki barcha muloqotlar bitta umumiy kalit bilan shifrlanadi. Bundan tashqari, WPA2 ishlatilganda hujumchi parolni buzishga urinishi mumkin — u avtomatik tarzda barcha mumkin bo‘lgan parollarni sinab ko‘rib, to‘g‘risini aniqlaguncha davom etadi.

Adabiyotlar tahlili

Yangi xavfsizlik standarti — Wireless Protected Access 3 (WPA3) bilan simsiz tarmoqlar ancha xavfsizroq bo‘ldi. Ilgari mavjud bo‘lgan passiv hujumlar, masalan, yashirincha kuzatish (eavesdropping), endi amalga oshirilmaydi. Bunga sabab, ochiq tarmoqlarda Opportunistic Wireless Encryption (OWE) va himoyalangan tarmoqlarda Simultaneous Authentication of Equals (SAE) texnologiyalarining joriy etilishidir. Bu orqali har bir mijoz va kirish nuqtasi o‘zaro yagona maxfiy kalit yaratib, ma’lumotlar aynan shu kalit orqali shifrlanadi.

SAE texnologiyasi hujumchiga juda tezkor parol sinovlarini amalga oshirish imkonini bermaydi. Bundan tashqari, SAE har bir parolni sinash vaqtida hujumchining onlayn bo‘lishini talab qiladi va urinishlar sonini chegaralash imkonini beradi. Bu esa parolni buzishni deyarli imkonsiz holga keltiradi.

Simsiz tarmoqlar uchun birinchi standart joriy etilganiga yigirma yildan oshdi [1], va shu vaqtdan buyon ular keng ommalashdi. Biroq, bu mashhurlik salbiy oqibatlarga ham olib

keldi — xususan, hujumchilar uchun zararli harakatlar qilish imkoniyati kengaydi. Bu hujumlarning oldini olish uchun xavfsizlik choralariga ehtiyoj paydo bo‘ldi.

2004-yildan boshlab, Wireless Protected Access 2 (WPA2) WiFi xavfsizligi uchun asosiy standart sifatida ishlatilmoqda. Undan oldin esa, qisqa vaqt davomida Wired Equivalent Privacy (WEP) va Wireless Protected Access (WPA) protokollari qo‘llanilgan [2]. Ammo bu ikki xavfsizlik protokoli muhim zaifliklarga ega bo‘lgani sababli, tez orada ulardan voz kechildi. WEP — bu RC4 oqimli shifrlash algoritmi asosida ishlaydi. Uning asosiy muammolaridan biri shundaki, agar ochiq matndagi bitta bit o‘zgartirilsa, shifrlangan matnda ham aynan o‘sha bit o‘zgaradi. Yana bir zaiflik — RC4 initialization vector (IV) dan foydalanadi. Bu IVlarning 16 milliondan 9000 tasi juda zaif bo‘lib, bu millionlab ma’lumot paketlarini ushlagan holda, tarmoqdagi kalitni kriptotahlil orqali buzishga imkon beradi [3]. WPA protokoli WEPdagi muammolarni bartaraf etish uchun ishlab chiqilgan bo‘lsa-da, mavjud qurilmalar faqat firmware yangilanishi orqali yangi protokoldan foydalana olishi uchun WPAda yana RC4ga asoslangan TKIP (Temporal Key Integrity Protocol) ishlatilgan. TKIP bu aslida RC4 atrofida qurilgan himoya qobig‘idir. IVlar uzaytirilgan bo‘lsa-da, asosiy muammo RC4 haligacha mavjudligidir. Shuning uchun WPA ham parolni buzish hujumlariga qarshi zaif edi [4]. Vanhoef va Piessens TKIPdagi bir nechta zaifliklar real sharoitlarda ham hujum qilish imkonini berishini isbotlashgan [5].

WPA2 esa bu muammoni RC4 ni olib tashlash orqali hal qildi va uning o‘rniga AES (Advanced Encryption Standard) ni joriy etdi, bu ancha xavfsiz hisoblanadi. WPA2 uzoq vaqt xavfsiz deb hisoblangan. Biroq 2016-yilda KRACK (Key Re-installation Attack) hujumi aniqlangan [6]. Yana bir keng tarqalgan hujum turi — lug‘at hujumi (dictionary attack) bo‘lib, unda hujumchi barcha mumkin bo‘lgan belgi kombinatsiyalarini tezda sinab ko‘radi. Ushbu turdagi hujumlar sababli yangi xavfsizlik standarti ishlab chiqildi.

WPA3 — 2018-yilning yanvar oyida e’lon qilingan yangi xavfsizlik standarti. Garchi bu ishda hali ham WPA3 bilan bog‘liq zaifliklarga asoslangan hujumlar tahlil qilinsa-da, avval WPA2 bilan WPA3 o‘rtasidagi asosiy farqlarni ko‘rib chiqish kerak bo‘ladi. Uchala WPA standarti to‘rt bosqichli kelishuv (four-way handshake) dan foydalanadi va bu aynan WPA3 dagi o‘zgarishlar sababli juda muhimdir. Shu bilan birga, mijoz va kirish nuqtasi (AP) o‘rtasida aloqa qanday o‘rnatilishini tushunish ham zarur. Shu sababli, simsiz tarmoqlarga umumiy qarab chiqiladi.

Metodologiya

Agar simsiz tarmoqda hech qanday xavfsizlik o‘rnatilmagan bo‘lsa, hujumchi tarmoq ustidan erkin kuzatuv olib borishi mumkin. U tarmoqqa ulanib, masalan, Wireshark kabi dastur yordamida tarmoqda uzatilayotgan ma’lumotlarni ushlaydi. Chunki hech qanday shifrlash yo‘q — barcha ma’lumotlar ochiq ko‘rinadi.

Agar tarmoq WPA2 xavfsizlik protokoli bilan himoyalangan bo‘lsa ham, hujumchi agar tarmoq a’zosi bo‘lsa, shunga o‘xshash tarzda kuzatuv olib borishi mumkin. Chunki WPA2’da barcha foydalanuvchilar bir xil shifrlash kalitlaridan foydalanadi. Bu esa tarmoqdagi istalgan foydalanuvchi tomonidan barcha ma’lumotlar shifri ochilishi mumkin degani.

Natijalar va muhokama

Parolni buzish (Password Cracking)

Agar tarmoq parol bilan himoyalangan bo‘lsa, hujumchi ushbu parolni topishga harakat qiladi. U har xil belgi kombinatsiyalarini sinab ko‘rish orqali parolni aniqlashga urinadi. Buni yanada samaraliroq qilish uchun u avval eng ko‘p ishlatiladigan yoki standart parollarni sinab ko‘radi. Ushbu parollar “dictionary” (lug‘at) deb ataladigan faylga joylashtiriladi va hujumchi dastur yordamida ularni avtomatik tarzda sinab chiqadi. Bu lug‘at hujumi (dictionary attack) deb ataladi. Agar tarmoq WPA2 bilan himoyalangan bo‘lsa, hujumchi to‘rt bosqichli kelishuv (handshake) xabarlarining bir nechtasini ushlashi kifoya. Agar hujumchi barcha to‘rtta xabarni to‘liq ushlagan bo‘lsa, u keyinchalik bu ma’lumotlar asosida offline rejimda lug‘atdagi parollarni sinab ko‘rishni boshlaydi. Agar to‘g‘ri parol lug‘at faylida mavjud bo‘lsa — parol topiladi.

Soxta tarmoq hujumi

Bu hujumda hujumchi xalqaro (ommaviy) tarmoqni taqlid qiladi, ya’ni o‘z tarmog‘ini asl tarmoq nomi bilan ataydi. Masalan, poezdda ishlatilayotgan ochiq tarmoq holatida, hujumchi ham o‘sha poezdda bo‘lishi mumkin va u asl tarmoq bilan bir xil nomdagi tarmoq ochadi. Aytaylik, yangi mijoz internetga ulanishni xohlaydi, chunki u ishga bormasdan oldin xizmat xatlar yuborishi kerak. Qurilmada ikkita bir xil nomli tarmoq ko‘rinadi va u tasodifan hujumchining tarmog‘iga ulanadi. Har narsa normal ishlayotgandek ko‘rinsa-da, foydalanuvchi buni sezmaydi. Ammo shu vaqtda, uning email serveriga kirish uchun ishlatgan login ma’lumotlari hujumchiga o‘tadi, hatto yuborilgan ma’lumotlar o‘zgartirilishi ham mumkin.

Wireless Protected Access 3 (WPA3)

Endi simsiz tarmoqlar qanday ishlashini va ularga qarshi qanday hujumlar mumkinligini ko‘rib chiqqanimizdan so‘ng, endi WPA3 protokolini muhokama qilamiz. Unda qanday hujumlar endi amalga oshirib bo‘lmaydi va eng muhimi, qanday hujumlar hali ham mumkinligini ko‘rib chiqamiz. Avvalo, WPA3’da qanday o‘zgarishlar kiritilganini va bu qanday qilib xavfsizlikni oshirganini ko‘rib chiqish lozim. Shuningdek, ushbu yangi standartni joriy etish holatini ham tahlil qilamiz va uning keng tarqalish muddati haqida ma’lumot beramiz. Yuqorida biz autentifikatsiya va assotsiatsiya bosqichlari, to‘rt bosqichli kelishuv (handshake) va ma’lumotlarni shifrlash qanday amalga oshirilishini WPA2 doirasida ko‘rib chiqdik. Biroq, bu jarayonlar WPA3’da ham ishlatiladi, faqat bir nechta kichik o‘zgarishlar va qo‘shimchalar bilan. Biz buni quyida

WPA3 ning ikki asosiy tushunchasini koʻrib chiqayotganimizda koʻramiz: Opportunistic Wireless Encryption (OWE) va Simultaneous Authentication of Equals (SAE).

Ushbu ikkala mexanizmda ham diskret logarifm masalasi (Discrete Logarithm Problem) juda muhim rol oʻynaydi. Bu matematik muammo yuqorida muhokama qilingan va u WPA3'da xavfsizlikning asosiy tayanchlaridan biri hisoblanadi. Endi biz WPA3 dagi oʻzgarishlarni koʻrib chiqqanimizdan keyin, avvalgi bobda muhokama qilingan hujumlarga bu oʻzgarishlar qanday ta'sir qilganini koʻrishimiz mumkin: Yashirin kuzatish u hujumni ochiq (himoyasiz) tarmoqlarda hamda WPA2 bilan himoyalangan tarmoqlarda amalga oshirish mumkin. WPA3 da esa ochiq tarmoqlar uchun OWE (Opportunistic Wireless Encryption) ishlatiladi. Bu shuni anglatadiki, barcha ma'lumotlar Diffie-Hellman kalit almashinuvi orqali yaratilgan umumiy maxfiy kalit yordamida shifrlanadi. Shuning uchun, hujumchi tarmoqda yuborilgan xabarlarning mazmunini koʻra olmaydi. WPA2 da esa hujumchi tarmoq ichida boʻlsa va parolni bilsa, barcha foydalanuvchilar bir xil shifrlash kalitidan foydalangani sababli, ma'lumotlarni oʻqib olish mumkin boʻladi. WPA3 (aniqrogʻi SAE) yordamida esa har bir aloqa uchun alohida maxfiy kalit yaratiladi va ma'lumotlar aynan shu maxfiy kalit bilan shifrlanadi. Shuning uchun tinglab olish mumkin boʻlmaydi.

Parolni buzish - bu esa WPA3 da SAE (Simultaneous Authentication of Equals) tufayli bu hujum amalga oshmaydi degani. Hujumchi har safar parolni tekshirishga urinayotganida, butun SAE protokoli bajarilishi kerak, bu esa ancha vaqt talab qiladi. Shu sababli, koʻp sonli parollarni ketma-ket sinab koʻrish juda koʻp vaqt oladi va amaliy jihatdan foydasiz boʻlib qoladi. WPA2 da esa hujumchi 4 bosqichli kelishuv (handshake) paketlarini yozib olib, oflayn rejimda parolni sinab koʻrishi mumkin boʻladi. Ammo SAE da bu mumkin emas – har bir parol taxmini real vaqtda tarmoqqa yuborilishi kerak. Shuningdek, tarmoq hujumchining necha marta urinish qilayotganini nazorat qilib, urinishlar soniga cheklov qoʻyishi ham mumkin.

WPA3 yuqoridagi hujumlarni yoʻqqa chiqargani holda, bu turdagi hujumga qarshi hech qanday yechim bermaydi.

Ya'ni, kimdir hanuzgacha soxta tarmoq yaratib, oʻzini ishonchli haqiqiy tarmoqdek koʻrsatishi mumkin. Masalan, biror poyezd ichidagi ochiq Wi-Fi tarmogʻiga oʻxshash nomli tarmoq ochiladi. Foydalanuvchi esa notoʻgʻri tarmoqqa ulanib, oʻz ma'lumotlarini hujumchiga oshkor qilganini sezmaydi. WPA3 bu muammoni hal qilmagan. Shu sababli, biz bu tatqiqot ishida ushbu hujumga qarshi yechim taklif qilamiz.

"evil twin attack" hujumlariga qarshi himoya

Ushbu ishda biz avval bu muammoning mohiyatiga chuqurroq nazar tashlaymiz. Oldingi ishda OWE (Opportunistic Wireless Encryption) ochiq tarmoqlar uchun yaxshiroq xavfsizlikni ta'minlashi haqida

ma’lumot, ammo u barcha muammolarni hal qilmaydi. Hali ham saqlanib qolayotgan muammo bu “evil twin attack” – “evil twin attack”. Bu hujumda biror shaxs ochiq Wi-Fi tarmog‘ining anatomik nomiga ega bo‘lgan soxta tarmoqni xuddi o‘sha joyda ochib, foydalanuvchilarni chalkashtiradi. Foydalanuvchi bu ikki tarmoqni ajrata olmagani uchun, tasodifan yovuz niyatli tarmoqqa ulanib qoladi. Natijada zararlanuvchi bilan hujumchi o‘rtasida ma’lumot kalitlari almashiladi va hujumchi yuborilayotgan va olinayotgan ma’lumotlarni shifrdan chiqarib o‘qiy oladi. Yaxshiyamki, ilovalar (apps) TLS (Transport Layer Security) yordamida server bilan bo‘layotgan aloqani shifrlab yuborishi mumkin. Ammo, hamma saytlar va ilovalar TLS’dan foydalanmaydi. Bu holatda, foydalanuvchining login-parollari hujumchining tarmog‘i orqali o‘tadi, bu esa katta xavf tug‘diradi. Hujumchi, ishonchli tarmoqdek harakat qilib, shifrlangan ma’lumotni yechadi, tekshiradi va muhim ma’lumotlarni izlaydi. Hatto agar parol matn ko‘rinishida yuborilmasa, balki hash holatda yuborilsa ham, hujumchi hash qiymatini saqlab qoladi va kerak bo‘lganda serverga yuborib, tizimga kira oladi.Bundan ham yomoni, bir xil paroldan bir nechta servislar uchun foydalanadigan foydalanuvchilar juda ko‘p. Shunday qilib, kichik bir servisdagi hisob ma’lumotlari orqali katta tizimlarga ham kirish mumkin bo‘ladi.

Simsiz tarmoqlardagi hujumlar

Simsiz tarmoqlar qanday ishlashini ko‘rib chiqqanimizdan so‘ng, bu tarmoqlarga qarshi, bo‘lishi mumkin bo‘lgan hujumlarni ko‘rib chiqamiz. Eng muhim hujumlar quyidagilar:

Yashirin kuzatish (Eavesdropping): Agar simsiz tarmoqda hech qanday xavfsizlik choralari bo‘lmasa, hujumchi tarmoqni kuzatishi mumkin. U tarmoqqa ulanadi va Wireshark kabi vosita yordamida tarmoqdagi uzatilayotgan ma’lumotlarni tutib oladi. Agar tarmoqda xavfsizlik yo‘q bo‘lsa, bu ma’lumotlarni osongina ko‘rish mumkin. Agar WPA2 xavfsizligi qo‘llanilsa, hujumchi tarmoq a’zosi bo‘lsa, u xuddi shu ishni qila oladi. WPA2 tarmog‘ida barcha qurilmalar bir xil shifrlash kalitlaridan foydalanadi, bu esa yovuz niyatdagi foydalanuvchiga barcha ma’lumotlarni ochish imkonini beradi.

Parolni buzish (Password cracking): Agar tarmoq parol bilan himoyalangan bo‘lsa, hujumchi bu parolni topishga harakat qilishi mumkin. U har xil belgilar kombinatsiyalarini sinab ko‘rishi mumkin. Avval mashhur yoki odatiy parollarni o‘z ichiga olgan "lug‘at"dan foydalaniladi – bu lug‘at bo‘yicha avtomatik sinov o‘tkaziladi, bu lug‘atli hujum (dictionary attack) deb ataladi. Agar WPA2 ishlatilsa, hujumchi 4 bosqichli handshake jarayonining ma’lumotlarini ushlab olib, keyinchalik oflayn tarzda parolni buzishga urinishi mumkin.

Evil twin attack: Hujumchi ishonchli tarmoq sifatida ko‘rinishga

ega bo‘lgan tarmoqni yaratishi mumkin. Masalan, lokal tarmoqda ochiq tarmoq mavjud bo‘lsa, hujumchi aynan shu tarmoqni buzishi mumkin. Foydalanuvchi ushbu ikki tarmoq orasidan hujumchi nikini tanlashi mumkin. Bu holatda foydalanuvchi o‘z elektron pochta serveriga ulanish uchun kerakli ma’lumotlarni yuboradi va bu ma’lumotlar hujumchiga o‘tadi.

WPA3 – Wireless Protected Access 3

Endi biz simsiz tarmoqlar qanday ishlashini va ularga qanday hujumlar mumkinligini ko‘rib chiqqanimizdan so‘ng, WPA3 qanday o‘zgarishlar olib kelganini va u qaysi hujumlarga yechim berishini ko‘rib chiqamiz.

WPA3'ning ikkita asosiy konsepti mavjud:

OWE – Opportunistic Wireless Encryption: Bu ochiq tarmoqlarda avtomatik shifrlashni ta’minlaydi.

SAE – Simultaneous Authentication of Equals: Bu esa kuchli parolga asoslangan autentifikatsiyani taklif etadi.

Har ikkala usul diskret logarifm masalasiga asoslangan. Bu matematik muammo shifrlashni kuchaytirishda muhim rol o‘ynaydi.

Xulosa

Ushbu maqolada shuni xulosa qilish mumkinki, Wireless Protected Access 3 (WPA3), ayniqsa Simultaneous Authentication of Equals (SAE) va Opportunistic Wireless Encryption (OWE) simsiz tarmoqlarda xavfsizlikni sezilarli darajada oshiradi. Biroq, xavfsizlik darajasi hali mukammal emasligini va yovuz egizak (evil twin) hujumiga alohida e’tibor qaratilganini ko‘riladi, chunki WPA3 da yovuz egizak hujumlariga qarshi hech qanday o‘zgarishlar yo‘q. Bu hujumlarga bir nechta qarshi yechimlar mavjud, masalan sertifikatlar, statik tarmoq nomlari, jamoaviy kalit tarmoq nomi sifatida va birinchi ulanishga ishonch (Trust on First Use) kabilar. Sertifikatlardan foydalanish aniq yechim sifatida ko‘rish mumkin, chunki biz uni veb-brauzerda ishlatamiz, lekin bu simsiz tarmoqlar holatida ishlamaydi. Aksincha, “birinchi ulanishga ishonch”ni eng yaxshi variant deb xulosa qilsa bo‘ladi va bu yondashuvni amalga oshirishni va turli xil holatlarda qanday ishlashini tushunish mumkin. Joriy amalga oshirilgan tarmoqni qo‘llash bilan birga, to‘rt bosqichli handshake vaqtida ba’zi qo‘shimcha ma’lumotlar yuborilishi kerak. Bu taklif qilgan yechimni WPA3 bilan yoki kelajakda chiqqan standartlardan biri bilan birgalikda amalga oshirish uchun ishlatilishi mumkin.

Foydalanilgan adabiyotlar ro'yxati:

1. Wi-Fi Alliance. Certification, 2019. [Online; accessed May 23, 2019]. URL: https://www.wi-fi.org/certification.

2. Joeri de Ruiter. Advanced network security: Wifi security, 2018. [Lec ture slides Master course Advanced Network Security from the master Cyber Security].

3. Paramvir Bahl, Ranveer Chandra, Jitendra Padhye, Lenin Ravin dranath, Manpreet Singh, Alec Wolman, and Brian Zill. Enhancing the security of corporate wi-fi networks using dair. In Proceedings of the 4th international conference on Mobile systems, applications and services, pages 1–14. ACM, 2006.

4. Sharon Boeyen, Stefan Santesson, Tim Polk, Russ Housley, Stephen Farrell, and Dave Cooper. Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. RFC 5280, May 2008. URL: https://rfc-editor.org/rfc/rfc5280.txt, doi:10.17487/RFC5280.

5. Nancy Cam-Winget, Russ Housley, David Wagner, and Jesse Walker. Security flaws in 802.11 data link protocols. Communications of the ACM, 46(5):35–39, 2003.

6. CheapSSLSecurity. What is ssl tls handshake understand the process in just 3 minutes, 2019. [Online; accessed May 23, 2019]. URL: https://cheapsslsecurity.com/blog/what-is-ssl-tls-handshake-understand-the-process-in-just-3-minutes/.

Ingliz tili muharriri: *Nosirova Nargiza Jamoliddin qizi*
Musahhih: *Vahobova Marfua Mirkamalovna*
Sahifalovchi va dizayner: *Zoirov Sardor Ziyodin o'g'li*

1-maxsus son

© Materiallar ko‘chirib bosilganda **“Management and Economics Scientific Research Journal”** jurnali manba sifatida ko‘rsatilishi shart. Jurnalda bosilgan material va reklamalardagi dalillarning aniqligiga mualliflar ma’sul. Tahririyat fikri har vaqt ham mualliflar fikriga mos kelamasligi mumkin. Tahririyatga yuborilgan materiallar qaytarilmaydi.

Mazkur jurnalda maqolalar chop etish uchun quyidagi havolalarga maqola, reklama, hikoya va boshqa ijodiy materiallar yuborishingiz mumkin.
Materiallar va reklamalar pullik asosda chop etiladi.
El. pochta: journals@timeedu.uz
Tel.: +998 95 651 90 00

“Management and Economics Scientific Research Journal” jurnali 19.09.2024-yildan O‘zbekiston Respublikasi Prezidenti Adminstratsiyasi huzuridagi Axborot va ommaviy kommunikatsiyalar agentligi tomonidan 404368-son reyestr raqami tartibi bo‘yicha ro‘yxatdan o‘tkazilgan. Litsenziya raqami: C-5669639
PNFL: 308906510

Manzilimiz: *Toshkent shahar, Yakkasaroy tumani*
Shota Rustaveli ko'chasi, 114