WPA3 XAVFSIZLIK PROTOKOLI VA ZAIFLIKLARI

WPA3 SECURITY PROTOCOL AND ITS VULNERABILITIES

ПРОТОКОЛ БЕЗОПАСНОСТИ WPA3 И ЕГО УЯЗВИМОСТИ

Sobirjonov Behzodbek Qahramon o‘gli
Farg‘ona davlat universiteti Axborot texnologiyalari kafedrasi o‘qituvchisi
behzodbekqahramonovich@gmail.com
Nishonov Abbosbek Qahramonjon o’g’li
Farg‘ona davlat universiteti Axborot tizimlari va texnologiyalari yo’nalishi 2-kurs talabasi
abbosbeknishonov00631@gmail.com

Annotatsiya. WPA3 (Wi-Fi Protected Access 3) simsiz tarmoqlarni himoya qilish uchun eng so'nggi va eng ilg'or xavfsizlik protokoli hisoblanadi. U WPA2 ga nisbatan sezilarli yaxshilanishlarni, jumladan, kuchliroq shifrlash va yangi Simultaneous Authentication of Equals (SAE) qo'l berish mexanizmini taqdim etadi. Ushbu maqola WPA3 protokolining asosiy xavfsizlik xususiyatlarini, jumladan, oldinga maxfiylikni va kuchli parollarni himoya qilishni chuqur tahlil qiladi. Shuningdek, u WPA3 ning ma'lum bo'lgan zaifliklarini, masalan, "Dragonfly" hujumlariga nisbatan sezgirlikni va amalga oshirishdagi potentsial kamchiliklarni ko'rib chiqadi. Maqola WPA3 ning afzalliklari va cheklovlarini tushunishning muhimligini ta'kidlaydi, bu esa simsiz tarmoq xavfsizligini yanada mustahkamlashga yordam beradi.

Kalit so‘zlar: WPA3, Xavfsizlik protokoli, Zaifliklar, Simsiz tarmoq, SAE, Shifrlash, Dragonfly hujumi, Tarmoq xavfsizligi

Abstract. WPA3 (Wi-Fi Protected Access 3) represents the latest and most advanced security protocol for protecting wireless networks. It introduces significant improvements over its predecessor, WPA2, including stronger encryption and the new Simultaneous Authentication of Equals (SAE) handshake mechanism. This article provides an in-depth analysis of WPA3 protocol's core security features, such as forward secrecy and enhanced password protection. Furthermore, it examines known vulnerabilities and potential weaknesses associated with WPA3, including its susceptibility to "Dragonfly" attacks and implementation flaws. The paper emphasizes the critical importance of understanding both the strengths and limitations of WPA3 to further bolster wireless network security.

Keywords: WPA3, Security protocol, Vulnerabilities, Wireless network, SAE, Encryption, Dragonfly attack, Network security

Аннотация. WPA3 (Wi-Fi Protected Access 3) является новейшим и наиболее продвинутым протоколом безопасности для защиты беспроводных сетей. Он предлагает значительные улучшения по сравнению с WPA2, включая более надежное

шифрование и новый механизм рукопожатия Simultaneous Authentication of Equals (SAE). Данная статья представляет углубленный анализ ключевых функций безопасности протокола WPA3, таких как прямая секретность и улучшенная защита паролей. Кроме того, в ней рассматриваются известные уязвимости и потенциальные недостатки, связанные с WPA3, включая его подверженность атакам "Dragonfly" и возможные ошибки реализации. Работа подчеркивает критическую важность понимания как преимуществ, так и ограничений WPA3 для дальнейшего укрепления безопасности беспроводных сетей.

Ключевые слова: WPA3, Протокол безопасности, Уязвимости, Беспроводная сеть, SAE, Шифрование, Атака Dragonfly, Сетевая безопасность

KIRISH

Bugungi kunda axborot texnologiyalarining jadal rivojlanishi natijasida simsiz tarmoqlardan foydalanish kundalik hayotning ajralmas qismiga aylandi. Internetga ulanishning qulay va tezkor usuli sifatida Wi-Fi texnologiyasi uy, ta’lim muassasalari, korxonalar hamda davlat tashkilotlarida keng qo‘llanilmoqda. Biroq simsiz tarmoqlarning ommalashuvi bilan bir qatorda, kiberxavfsizlik bilan bog‘liq tahdidlar ham ortib bormoqda. Tarmoqqa ruxsatsiz kirish, ma’lumotlarni o‘g‘irlash, foydalanuvchi shaxsiy ma’lumotlarini qo‘lga kiritish kabi xavflar Wi-Fi tarmoqlarini himoyalash zaruratini yanada kuchaytirdi.

Simsiz tarmoqlar xavfsizligini ta’minlash maqsadida turli himoya protokollari ishlab chiqilgan bo‘lib, ular orasida WPA (Wi-Fi Protected Access) oilasiga kiruvchi standartlar alohida o‘rin egallaydi. Dastlabki WEP protokolidagi kamchiliklardan so‘ng WPA va WPA2 standartlari ishlab chiqilgan bo‘lsa-da, vaqt o‘tishi bilan ularda ham turli zaifliklar aniqlangan. Ayniqsa, WPA2 protokolida aniqlangan KRACK hujumi kabi zaifliklar yanada mukammal va xavfsiz himoya mexanizmini yaratish zaruratini yuzaga keltirdi. Shu sababli Wi-Fi Alliance tashkiloti tomonidan yangi avlod xavfsizlik standarti — WPA3 protokoli taqdim etildi.

WPA3 protokoli foydalanuvchilarning ma’lumotlarini yanada ishonchli himoyalash, kuchsiz parollarga qarshi himoyani kuchaytirish hamda ochiq tarmoqlarda ma’lumotlar maxfiyligini ta’minlash kabi bir qator yangi imkoniyatlarni o‘z ichiga oladi.

Asosiy qism

WPA3 xavfsizlik protokoli simsiz tarmoqlarda ma’lumotlarni himoyalashning zamonaviy usullaridan biri hisoblanadi. Ushbu protokol Wi-Fi tarmoqlarida foydalanuvchi ma’lumotlarining maxfiyligi, yaxlitligi va xavfsizligini ta’minlash maqsadida ishlab chiqilgan. WPA3 avvalgi WPA va WPA2 standartlariga nisbatan takomillashtirilgan bo‘lib, kuchli autentifikatsiya hamda zamonaviy shifrlash mexanizmlarini o‘z ichiga oladi. Protokol foydalanuvchilarni ruxsatsiz kirish, parolni taxmin qilish va ma’lumotlarni ushlab qolish kabi kiberhujumlardan himoya qilishga xizmat qiladi.

WPA3 protokolining ishlash prinsipi

WPA3 protokolining ishlash prinsipi asosan SAE (Simultaneous Authentication of Equals) autentifikatsiya mexanizmiga asoslanadi. Ushbu mexanizm foydalanuvchi va kirish nuqtasi o‘rtasida xavfsiz bog‘lanish hosil qiladi. SAE texnologiyasi orqali har bir ulanish uchun alohida kalit yaratiladi va bu parolni qayta tiklash yoki lug‘at hujumlari orqali aniqlash ehtimolini kamaytiradi. Natijada tarmoq xavfsizligi sezilarli darajada oshadi.

Asosiy ishlash bosqichlari

Autentifikatsiya jarayoni — foydalanuvchi qurilmasi va Wi-Fi router o‘rtasida xavfsiz identifikatsiya amalga oshiriladi. Ushbu bosqichda SAE algoritmi yordamida maxfiy kalitlar almashinuvi bajariladi.

Shifrlash jarayoni — uzatilayotgan ma’lumotlar zamonaviy kriptografik algoritmlar yordamida shifrlanadi. Bu uchinchi shaxslarning ma’lumotlarni o‘qishini cheklaydi.

Xavfsiz ulanish yaratish — foydalanuvchi tarmoqqa muvaffaqiyatli ulangandan so‘ng individual sessiya kaliti hosil qilinadi va ma’lumot almashinuvi himoyalangan holda davom etadi.

Ochiq tarmoqlarni himoyalash — Opportunistic Wireless Encryption (OWE) texnologiyasi orqali ochiq Wi-Fi tarmoqlarida ham ma’lumotlar avtomatik ravishda shifrlanadi.

WPA3 protokolining afzalliklari

WPA3 protokolining muhim afzalliklaridan biri kuchsiz parollarga qarshi himoyaning kuchaytirilganidir. Avvalgi WPA2 protokolida hujumchilar maxsus dasturlar yordamida parollarni taxmin qilish imkoniga ega bo‘lgan bo‘lsa, WPA3 da bunday hujumlarning samaradorligi ancha kamaytirilgan. Bundan tashqari, korporativ tarmoqlar uchun 192 bitli xavfsizlik rejimining joriy etilishi yuqori darajadagi himoyani ta’minlaydi.

WPA3 protokolining zaifliklari

Shunga qaramasdan, WPA3 protokolida ham ayrim zaifliklar mavjudligi aniqlangan. Tadqiqotchilar tomonidan aniqlangan Dragonblood hujumlari SAE autentifikatsiya mexanizmidagi ayrim kamchiliklarni ko‘rsatib berdi. Ushbu hujumlar yordamida tajovuzkor autentifikatsiya jarayonini tahlil qilish yoki foydalanuvchi paroli haqida ma’lumot olishga harakat qilishi mumkin.

Zaifliklarning asosiy turlari

Downgrade attack — qurilmani xavfsizligi pastroq protokollarga o‘tishga majbur qilish orqali himoya darajasini kamaytirish.

Side-channel attack — autentifikatsiya jarayonidagi vaqt yoki hisoblash jarayonlarini tahlil qilish orqali maxfiy ma’lumotlarni aniqlashga urinish.

DoS hujumlari — tarmoq faoliyatini izdan chiqarish va foydalanuvchilar ulanishiga to‘sqinlik qilish.

Xavfsizlikni ta’minlash usullari

WPA3 xavfsizligini oshirish uchun qurilmalarni muntazam yangilash, murakkab parollardan foydalanish va eski xavfsizlik standartlarini o‘chirib qo‘yish tavsiya etiladi. Shu

bilan birga, tarmoq administratorlari xavfsizlik monitoringini doimiy ravishda amalga oshirib borishlari zarur.

Xulosa

WPA3 protokoli simsiz tarmoqlar xavfsizligini WPA2 ga nisbatan sezilarli darajada oshirgan eng so‘nggi standartdir. Uning SAE mexanizmi oflayn lug‘at hujumlarining oldini olib, kelajak maxfiyligini ta’minlaydi, Enhanced Open esa ochiq tarmoqlarda shifrlashni joriy etadi. Biroq, ushbu tadqiqot WPA3 ning arxitekturasi va ilg‘or kriptografik yondashuvlarini tahlil qilar ekan, uning o‘zida ham, ayniqsa SAE amalga oshirilishida va IoT integratsiyasida ma’lum zaifliklar mavjudligini ko‘rsatdi. Maqola aniqlangan kamchiliklarni bartaraf etish bo‘yicha amaliy tavsiyalar berib, Wi-Fi xavfsizligi sohasida doimiy tadqiqotlar va protokolni muntazam yangilash zarurligini ta’kidlaydi. Bu esa kelajakdagi tahdidlarga qarshi mustahkam himoyani ta’minlash uchun muhimdir.

FOYDALANILGAN ADABIYOTLAR:

1.Vanhoef, M., Ronen, E. Dragonblood: WPA3'ning SAE qo'l siqish protokolini tahlil qilish. 29-chi USENIX Xavfsizlik Simpoziumi (USENIX Security 20) materiallari, 2020. – https://www.usenix.org/conference/usenixsecurity20/presentation/vanhoef

2. Kazama, M., Kakizaki, K., Kiyomoto, S. PMKID sizishi orqali WPA3-Personal'ga qarshi amaliy hujum. IEICE Transactions on Communications, E104.B(11), 1269-1277-betlar, 2021. – https://www.jstage.jst.go.jp/article/transcom/E104.B/11/E104.B_1269/_article/-char/ja/

3. Al-Mekhlafi, A. G., Al-Mekhlafi, A. S., Al-Mekhlafi, A. A., Al-Mekhlafi, A. A. WPA3 xavfsizlik protokoli va uning zaifliklari bo'yicha keng qamrovli tadqiqot. 2022 Xalqaro Kompyuter Fanlari va Muhandislik Konferensiyasi (ICCSE), 2022, 1-6-betlar. – https://ieeexplore.ieee.org/document/9963668

4. Kim, J., Kim, J., Kim, H. WPA3-Personal qo'l siqish protokoliga qarshi yon kanal hujumi. 2021 Xalqaro Axborot Tarmoqlari Konferensiyasi (ICOIN), 2021, 1-6-betlar. – https://ieeexplore.ieee.org/document/9330921

5. Karimov A.B., Sobirov D.E. Simsiz Wi-Fi tarmoqlarida ma'lumotlar xavfsizligini ta'minlashning dolzarb masalalari. Axborot Texnologiyalari va Kommunikatsiyalari Muammolari, Toshkent Axborot Texnologiyalari Universiteti, 2022, №3, 45-52-betlar.

6. Rahmatullayev F.X., G'aniyev U.N. Kriptografik protokollarning simsiz aloqa tizimlaridagi xavfsizlikni ta'minlashdagi o'rni. O'zbekiston Fanlar Akademiyasi Axborotnomasi, O'zbekiston Fanlar Akademiyasi, 2021, №5, 78-85-betlar.

7. Saidov J.M., Aliyev S.R. Wi-Fi tarmoqlarida autentifikatsiya mexanizmlarining tahlili va ularning zaifliklari. Toshkent Axborot Texnologiyalari Universiteti Ilmiy-texnik jurnali, Toshkent Axborot Texnologiyalari Universiteti, 2023, №1, 33-40-betlar.

8. Ergashev N.A., Qodirov B.I. Tarmoq xavfsizligida zamonaviy himoya protokollarini qo'llash samaradorligi. Milliy Universitet Xabarlari, O'zbekiston Milliy Universiteti, 2020, №4, 61-68-betlar.