WPA3 xavfsizlik protokoli va uning zaifliklari
Протокол безопасности WPA3 и его уязвимости
WPA3 security protocol and its vulnerabilities

Behzod Sobirjonov Qahramonivich
FarDu Axborot tehnologiyalari
kafedrasi o‘qituvchisi
behzodbekqahramonovich@gmail.com
Sharofiddinov Shahobiddin Norinboy o’g’li
FarDu Axborot tizimlari va texnologiyalari
yo‘nalishi 2-bosqich talabasi
sharofiddinovshahobiddin908@gmail.com
Telefon raqam:88-211-30-99

Annotatsiya: Ushbu maqolada simsiz tarmoqlarda xavfsizlikni ta’minlash uchun ishlab chiqilgan WPA3 (Wi-Fi Protected Access 3) protokolining ishlash mexanizmlari, uning ilg‘or kriptografik yondashuvlari hamda mavjud zaifliklari tahlil qilinadi. Maqolada WPA3 protokolining avvalgi WPA2 standartiga nisbatan ustunliklari, autentifikatsiya jarayonidagi yangiliklar va hujumlarga qarshi chidamlilik darajasi ko‘rib chiqiladi. Shuningdek, zamonaviy tadqiqotlar asosida aniqlangan zaif tomonlar va ularni kamaytirish bo‘yicha tavsiyalar beriladi.

Kalit so‘zlar: Kiberxavfsizlik, WPA3, Wi-Fi xavfsizligi, SAE autentifikatsiyasi, Kriptografiya, Tarmoq himoyasi

Аннотация: В данной статье рассматриваются механизмы работы протокола безопасности WPA3, предназначенного для защиты беспроводных сетей, а также анализируются его уязвимости. Особое внимание уделяется криптографическим методам, преимуществам WPA3 по сравнению с WPA2 и устойчивости к современным кибератакам. Также рассматриваются выявленные исследователями слабые места протокола и предлагаются рекомендации по их устранению.

Ключевые слова: Кибербезопасность, WPA3, безопасность Wi-Fi, аутентификация SAE, криптография, защита сети

Abstract: This article examines the WPA3 (Wi-Fi Protected Access 3) security protocol, focusing on its operational mechanisms, advanced cryptographic approaches, and potential vulnerabilities. It analyzes the improvements over WPA2, particularly in authentication and resistance to cyberattacks. The paper also discusses recently discovered weaknesses and provides recommendations to mitigate associated risks.

Keywords: Cybersecurity, WPA3, Wi-Fi security, SAE authentication, Cryptography, Network protection

KIRISH

Zamonaviy axborot jamiyatida simsiz aloqa texnologiyalari, ayniqsa Wi-Fi tarmoqlari, kundalik hayotning ajralmas qismiga aylangan. Mobil qurilmalar, aqlli uy tizimlari, korporativ infratuzilmalar va ta’lim muassasalari faoliyati bevosita simsiz tarmoqlarga bog‘liq bo‘lib bormoqda. Bu esa uzatilayotgan ma’lumotlarning xavfsizligini ta’minlash masalasini yanada muhim va dolzarb

qilib qo‘yadi. Chunki ochiq muhitda ishlovchi simsiz tarmoqlar turli xil kiberhujumlar uchun nisbatan qulay nishon hisoblanadi.

Avvalgi yillarda Wi-Fi tarmoqlarini himoya qilishda keng qo‘llanilgan WPA2 protokoli ma’lum vaqt davomida ishonchli yechim sifatida xizmat qilgan bo‘lsa-da, vaqt o‘tishi bilan undagi zaifliklar aniqlanib, yangi tahdidlarga qarshi yetarli darajada himoya bera olmasligi ma’lum bo‘ldi. Ayniqsa, parolga asoslangan autentifikatsiya mexanizmlarining zaif tomonlari va trafikni tahlil qilish orqali amalga oshiriladigan hujumlar yangi, yanada mukammal xavfsizlik standartini ishlab chiqishni talab etdi.

Shu ehtiyoj natijasida yangi avlod simsiz xavfsizlik protokoli — WPA3 ishlab chiqildi. Ushbu protokol ilg‘or kriptografik yondashuvlarga asoslangan bo‘lib, foydalanuvchi autentifikatsiyasini kuchaytirish, ma’lumotlarni himoyalash va turli xil hujumlarga qarshi barqarorlikni oshirishga qaratilgan. Biroq, har qanday zamonaviy texnologiya singari, WPA3 ham mutlaq xavfsizlikni ta’minlay olmaydi va uning ayrim zaifliklari ilmiy tadqiqotlar jarayonida aniqlanmoqda.

Mazkur maqolada WPA3 xavfsizlik protokolining ishlash prinsiplari, uning avvalgi standartlarga nisbatan ustunliklari hamda aniqlangan zaifliklari tahlil qilinadi. Shuningdek, simsiz tarmoqlar xavfsizligini oshirishga qaratilgan amaliy tavsiyalar va zamonaviy yondashuvlar ko‘rib chiqiladi.

Zamonaviy raqamli infratuzilmalarda simsiz tarmoqlar muhim o‘rin egallaydi va ular orqali uzatilayotgan ma’lumotlarning xavfsizligi global muammo sifatida qaraladi. Ayniqsa, Wi-Fi texnologiyalarining keng tarqalishi bilan bir qatorda, ularning himoyasi ham takomillashib bormoqda. Shu jarayonda WPA3 xavfsizlik protokoli yangi bosqich sifatida joriy etildi. U nafaqat oldingi standartlarning kamchiliklarini bartaraf etishga, balki yanada kuchli kriptografik himoyani ta’minlashga qaratilgan.

WPA3 protokoli asosan autentifikatsiya va ma’lumotlarni shifrlash mexanizmlarini takomillashtirish orqali ishlaydi. Uning eng muhim yangiliklaridan biri — Simultaneous Authentication of Equals (SAE) algoritmidir. Ushbu mexanizm parolga asoslangan autentifikatsiya jarayonini kuchaytirib, offline brute-force hujumlariga qarshi samarali himoya yaratadi. WPA2 da qo‘llanilgan Pre-Shared Key (PSK) tizimidan farqli o‘laroq, SAE har bir autentifikatsiya urinishida yangi kriptografik kalitlar generatsiya qiladi. Bu esa hujumchilarga tarmoq trafikini yozib olib, keyinchalik uni buzish imkoniyatini deyarli yo‘qqa chiqaradi.

WPA3 shuningdek, “forward secrecy” tamoyilini qo‘llab-quvvatlaydi. Bu shuni anglatadiki, agar tarmoq kaliti biror vaqtda qo‘lga kiritilgan taqdirda ham, oldingi uzatilgan ma’lumotlarni dekodlash imkonsiz bo‘ladi. Bu esa ayniqsa korporativ va davlat darajasidagi tarmoqlar uchun muhim ahamiyat kasb etadi. Bundan tashqari, WPA3 ochiq tarmoqlar uchun Opportunistic Wireless Encryption (OWE) texnologiyasini joriy qilib, parolsiz Wi-Fi tarmoqlarida ham ma’lumotlarni shifrlash imkonini beradi.

Shunga qaramay, WPA3 mutlaq xavfsiz tizim emas. Amaliyotda aniqlangan ba’zi zaifliklar uning murakkabligi va implementatsiya xatolari bilan bog‘liq. Jumladan, “Dragonblood” nomi bilan tanilgan hujumlar to‘plami SAE protokolining ayrim implementatsiyalarida zaifliklar mavjudligini ko‘rsatdi. Bu hujumlar orqali tajovuzkor autentifikatsiya jarayonidagi vaqt kechikishlari yoki yon kanal (side-channel) ma’lumotlaridan foydalanib, parol haqida qisman ma’lumot olishga muvaffaq bo‘lishi mumkin.

Bundan tashqari, WPA3 ning ayrim qurilmalarda noto‘g‘ri sozlanishi yoki eski dasturiy ta’minot bilan ishlashi xavfsizlik darajasini pasaytiradi. Ko‘plab foydalanuvchilar hali ham

WPA2/WPA3 mixed mode rejimidan foydalanadi, bu esa yangi protokolning afzalliklarini to‘liq namoyon etmasligiga sabab bo‘ladi. Shu sababli, tizim administratorlari va foydalanuvchilar konfiguratsiya jarayoniga alohida e’tibor qaratishlari zarur.

WPA3 xavfsizlik protokoli simsiz tarmoqlarni himoya qilishda muhim qadam bo‘lishiga qaramay, uning samaradorligi to‘g‘ri sozlash va muntazam yangilanishlarga bog‘liq. Kiberxavfsizlik doimiy rivojlanayotgan soha bo‘lib, har qanday yangi texnologiya bilan birga yangi tahdidlar ham yuzaga keladi. Shu bois, WPA3 dan foydalanishda nafaqat uning texnik imkoniyatlarini bilish, balki aniqlangan zaifliklardan xabardor bo‘lish ham muhimdir.

Xulosa

WPA3 (Wi-Fi Protected Access 3) protokoli zamonaviy simsiz tarmoqlar xavfsizligini yangi bosqichga olib chiqish maqsadida ishlab chiqilgan bo‘lib, u o‘zidan oldingi WPA2 standartidagi ko‘plab fundamental kamchiliklarni bartaraf etishga qaratilgan. Ushbu protokolning eng asosiy ustunligi SAE (Simultaneous Authentication of Equals) deb ataladigan login almashish usulidir. Bu texnologiya "lug‘at hujumlari" (dictionary attacks) orqali parollarni buzib kirishni deyarli imkonsiz qiladi, chunki tajovuzkor tarmoq trafigini yozib olib, oflayn rejimda millionlab parollarni sinab ko‘rish imkoniyatidan mahrum bo‘ladi. Hatto foydalanuvchi oddiyroq parol tanlagan taqdirda ham, WPA3 uni himoya qilishda davom etadi.

Bundan tashqari, WPA3 protokoli ma’lumotlarni shifrlashda ancha kuchliroq bo‘lgan 192-bitli xavfsizlik rejimini taklif etadi, bu ayniqsa hukumat va yirik korporativ tarmoqlar uchun o‘ta muhimdir. Shuningdek, ochiq Wi-Fi tarmoqlarida (masalan, kafelarda) foydalanuvchilarning shaxsiy ma’lumotlarini himoya qilish uchun Opportunistic Wireless Encryption (OWE) texnologiyasi qo‘llaniladi. Bu foydalanuvchi parol kiritmagan holda ham u bilan router o‘rtasidagi trafikni individual ravishda shifrlash imkonini beradi. Biroq, mukammal xavfsizlik tizimi bo‘lmagani kabi, WPA3 ham o‘ziga xos zaifliklardan xoli emas. Protokol e’lon qilinganidan ko‘p o‘tmay, tadqiqotchilar Dragonblood deb nomlangan bir qator zaifliklarni aniqlashdi. Bu zaifliklar asosan SAE tizimidagi "mantiqiy xatolar" bilan bog‘liq bo‘lib, tajovuzkorlarga router protsessoriga haddan tashqari yuklama berish orqali xizmat ko‘rsatishni to‘xtatish (DoS) yoki parolni aniqlash uchun ma’lum bir yon kanalli hujumlarni amalga oshirishga yo‘l ochadi.

Foydalanilgan adabiyotlar

1. Vanhoef, M., Ronen, E. (2019). Dragonblood: Analyzing the Dragonfly Handshake of WPA3.
2. Wi-Fi Alliance. WPA3 Specification Documentation.
3. ISO/IEC 27001. Information Security Management Systems Requirements.
4. SANS Institute. Wireless Security and WPA3 Analysis Reports.