XAVFSIZLIK PROTOKOLLARI

ПРОТОКОЛ БЕЗОПАСНОСТИ WPA3 И ЕГО УЯЗВИМОСТИ

WPA3 SECURITY PROTOCOL AND ITS VULNERABILITIES

Sobirjonov Behzod Qahramon o‘g‘li
Farg‘ona davlat universiteti Axborot texnologiyalari kafedrasi katta o‘qituvchisi
behzodbekqahramonovich@gmail.com
Murodova Mahliyo Rashidjon qizi
Farg‘ona davlat universiteti Axborot tizimlari va texnologiyalar yo‘nalishi
2-kurs talabasi
mmahliyo2006@gmail.com

Annotatsiya

Ushbu maqolada zamonaviy simsiz tarmoqlarda keng qo‘llanilayotgan WPA3 xavfsizlik protokolining asosiy xususiyatlari, afzalliklari hamda mavjud zaifliklari tahlil qilinadi. Tadqiqot davomida WPA3 protokolining WPA2 ga nisbatan takomillashtirilgan jihatlari, xususan, autentifikatsiya jarayonining kuchaytirilgani, ma’lumotlarning ishonchli shifrlanishi va foydalanuvchi maxfiyligini ta’minlashdagi o‘rni yoritib beriladi. Shu bilan birga, protokolni amaliyotga joriy etish jarayonida yuzaga keladigan muammolar, xususan, noto‘g‘ri implementatsiya, moslik masalalari hamda Dragonblood turidagi hujumlar orqali yuzaga chiqadigan zaif tomonlar ham ko‘rib chiqiladi. Maqola yakunida WPA3 protokolining samaradorligini oshirish va xavfsizlik darajasini yanada mustahkamlash bo‘yicha tavsiyalar beriladi.

Kalit so‘zlar : *WPA3, simsiz tarmoq, xavfsizlik protokoli, autentifikatsiya, shifrlash, SAE, Dragonblood hujumi, zaifliklar, kiberxavfsizlik, ma’lumotlarni himoya qilish*

Аннотация

В данной статье анализируются основные характеристики, преимущества, а также существующие уязвимости современного протокола безопасности WPA3, широко применяемого в беспроводных сетях. В ходе исследования рассматриваются усовершенствованные аспекты WPA3 по сравнению с WPA2, в частности усиленный процесс аутентификации, надёжное шифрование данных и его роль в обеспечении конфиденциальности пользователей. Наряду с этим освещаются проблемы, возникающие при внедрении протокола на практике, включая ошибки реализации, вопросы совместимости, а также уязвимости, связанные с атаками типа

Dragonblood. В заключении статьи приводятся рекомендации по повышению эффективности WPA3 и дальнейшему укреплению уровня безопасности.

Ключевые слова : *WPA3, беспроводная сеть, протокол безопасности, аутентификация, шифрование, SAE, атака Dragonblood, уязвимости, кибербезопасность, защита данных*

Abstract

This article analyzes the main features, advantages, and existing vulnerabilities of the modern WPA3 security protocol, which is widely used in wireless networks. The study highlights the improvements of WPA3 compared to WPA2, particularly the enhanced authentication process, reliable data encryption, and its role in ensuring user privacy. At the same time, the paper examines challenges encountered during the practical implementation of the protocol, including implementation flaws, compatibility issues, and vulnerabilities associated with Dragonblood-type attacks. In conclusion, recommendations are provided to improve the effectiveness of WPA3 and further strengthen its security level.

Keywords : *WPA3, wireless network, security protocol, authentication, encryption, SAE, Dragonblood attack, vulnerabilities, cybersecurity, data protection*

Zamonaviy axborot texnologiyalari jadal rivojlanib borayotgan bir sharoitda simsiz tarmoqlarning ahamiyati tobora ortib bormoqda. Bugungi kunda Wi-Fi texnologiyalari nafaqat kundalik hayotda, balki ta’lim, sog‘liqni saqlash, sanoat va davlat boshqaruvi kabi muhim sohalarda ham keng qo‘llanilmoqda. Biroq simsiz tarmoqlarning ommalashuvi bilan bir qatorda, ularga nisbatan xavf-xatarlar va kiberhujumlar soni ham sezilarli darajada oshib bormoqda. Shu bois tarmoqlarda uzatilayotgan ma’lumotlarning maxfiyligi, yaxlitligi va mavjudligini ta’minlash dolzarb masalalardan biriga aylangan.

Avvalgi avlod xavfsizlik protokollari, xususan WPA2, uzoq vaqt davomida ishonchli himoya vositasi sifatida xizmat qilgan bo‘lsa-da, vaqt o‘tishi bilan undagi ayrim zaifliklar aniqlanib, yangi va yanada mukammal yechimlarni ishlab chiqishni taqozo etdi. Ana shunday ehtiyoj natijasida WPA3 xavfsizlik protokoli ishlab chiqildi. Ushbu protokol yanada kuchli autentifikatsiya mexanizmlari, yaxshilangan shifrlash usullari va foydalanuvchi ma’lumotlarini himoya qilishning ilg‘or yondashuvlari bilan ajralib turadi.

Shu bilan birga, har qanday texnologiya singari, WPA3 ham mutlaq mukammal emas va uni amaliyotga joriy etish jarayonida turli muammolar hamda zaifliklar yuzaga chiqishi mumkin. Mazkur maqolada aynan WPA3 protokolining imkoniyatlari, afzalliklari hamda mavjud zaif tomonlari atroflicha tahlil qilinadi.

Mazkur tadqiqot ishida WPA3 xavfsizlik protokolining amaliy jihatlari hamda uning zaifliklarini aniqlash maqsadida tajriba ishlari olib borildi.

1-rasm.WPA3 xavfsizlik rejimi sozlash oynasi

Tajriba muhiti sifatida WPA3 protokolini qo‘llab-quvvatlovchi simsiz tarmoq qurilmasi va Linux operatsion tizimiga ega kompyuter tanlandi. Tarmoq xavfsizligini tahlil qilish uchun maxsus dasturiy vositalardan foydalanildi.

Simsiz tarmoq qurilmasida xavfsizlik rejimi WPA3-Personal (SAE) holatiga o‘rnatildi va mustahkam parol belgilandi. Shundan so‘ng, tarmoqqa bir nechta qurilmalar ulanib, autentifikatsiya jarayoni kuzatildi. Trafik tahlili davomida SAE (Simultaneous Authentication of Equals) protokolining ishlash prinsipi o‘rganildi va uning WPA2 ga nisbatan yuqori darajadagi himoya ta’minlashi aniqlandi.

Keyingi bosqichda WPA3 protokoliga nisbatan aniqlangan zaifliklar amaliy jihatdan tekshirildi. Dragonblood attack hujumi doirasida autentifikatsiya jarayonidagi ayrim nozik jihatlar tahlil qilindi. Tajriba natijalariga ko‘ra, noto‘g‘ri sozlangan yoki yangilanmagan qurilmalarda ayrim zaifliklar yuzaga kelishi mumkinligi kuzatildi.

2-rasm.Routerga kabel orqali ulanish jarayoni

Himoya choralarining samaradorligi ham amaliy sinovdan o‘tkazildi. Jumladan, kuchli parollardan foydalanish, qurilma dasturiy ta’minotini muntazam yangilab borish va WPA3-only rejimini faollashtirish orqali xavfsizlik darajasini oshirish mumkinligi tasdiqlandi.

Olib borilgan amaliy tadqiqotlar natijasida WPA3 protokoli yuqori darajadagi himoya mexanizmlariga ega ekanligi, biroq ayrim implementatsiyalarda zaifliklar saqlanib qolishi mumkinligi aniqlandi.

Xulosa

Mazkur tadqiqot ishida WPA3 xavfsizlik protokolining zamonaviy simsiz tarmoqlardagi o‘rni, ishlash mexanizmlari hamda mavjud zaifliklari kompleks tarzda tahlil qilindi. Olib borilgan nazariy va amaliy izlanishlar natijasida WPA3 protokoli avvalgi avlod — WPA2 ga nisbatan sezilarli darajada takomillashtirilgan himoya mexanizmlariga ega ekanligi aniqlandi.

Autentifikatsiya jarayonida qo‘llaniladigan SAE mexanizmi parolni aniqlashga qaratilgan ko‘plab hujumlarga nisbatan yuqori darajadagi barqarorlikni ta’minlaydi. Shu bilan birga, amaliy tajribalar davomida ayrim holatlarda, ayniqsa noto‘g‘ri sozlangan yoki eskirgan qurilmalarda, xavfsizlik darajasining pasayishi kuzatilishi mumkinligi qayd etildi. Jumladan, Dragonblood attack doirasida aniqlangan zaifliklar protokolning ayrim implementatsiyalarida himoya mexanizmlarini chetlab o‘tish ehtimoli mavjudligini ko‘rsatadi.

WPA3 protokolining samaradorligi nafaqat uning nazariy jihatdan mukammalligiga, balki amaliy qo‘llanish jarayonida to‘g‘ri konfiguratsiya qilinishiga ham bevosita bog‘liq ekanligi ayon bo‘ladi. Xavfsizlikni maksimal darajada ta’minlash uchun foydalanuvchilardan kuchli parollardan foydalanish, qurilmalarni muntazam yangilab borish va zamonaviy himoya rejimlarini to‘liq faollashtirish talab etiladi.

WPA3 protokoli simsiz tarmoqlar xavfsizligini ta’minlashda muhim qadam bo‘lib, uning imkoniyatlaridan to‘liq va to‘g‘ri foydalanish axborot xavfsizligini mustahkamlashda muhim ahamiyat kasb etadi.

Foydalanilgan adabiyotlar

1. Wi-Fi Alliance. Wi-Fi CERTIFIED WPA3™ Security Overview. — 2018.
2. IEEE. IEEE 802.11 Wireless LAN Standards. — New York, 2020.
3. National Institute of Standards and Technology. Guidelines for Securing Wireless Local Area Networks (WLANs). — 2021.
4. Vanhoef Mathy, Ronen Eyal. Dragonblood: Analyzing the Dragonfly Handshake of WPA3 and EAP-pwd. — 2019.
5. Wireshark rasmiy hujjatlari va foydalanuvchi qo‘llanmasi. —
6. https://www.wireshark.org

7. Kali Linux. Penetration Testing Tools Documentation. — 2023.
8. Computer Networking: A Top-Down Approach / James F. Kurose, Keith W. Ross. — Pearson, 2021.