Scientific and Practical Cyber Security Journal (SPCSJ) 9(2): 36 – 40 ISSN 2587-4667 Scientific Cyber Security Association (SCSA)

WI-FI 6 SECURITY ANALYSIS: CHALLENGES AND PROTECTION MECHANISMS OF MODERN STANDARDS

Wi-Fi 6-ის უსაფრთხოების ანალიზი: თანამედროვე სტანდარტების გამოწვევები და დაცვის მექანიზმები

Sergei Simonovi[1,2], Nikoloz Trikishvili[1], Nikoloz Bajelidze[1], Irakli Macharashvili[1], Andria Gabadze[1], Nikoloz Kochlamazashvili[1]

[1]University of Young Penetration Testers, 1 Paata Saakadze St, Tbilisi 0102, Georgia

[2]Caucasus University, 1 Paata Saakadze St, Tbilisi 0102, Georgia

ABSTRACT: Wi-Fi 6, also known as IEEE 802.11ax, is the latest standard in wireless communication technologies, developed to address the growing demands of modern digital environments — particularly in scenarios where multiple devices require simultaneous and efficient network access. This standard not only enhances transmission speed and network throughput, but also incorporates advanced security mechanisms such as WPA3 (Wi-Fi Protected Access 3), SAE (Simultaneous Authentication of Equals), and PMF (Protected Management Frames), designed to mitigate vulnerabilities found in previous generations. The aim of this article is to analyze the security architecture of Wi-Fi 6, evaluate its response to current cyber threats, and highlight the technical features that support the standard's adaptability to today's cybersecurity challenges.

KEYWORDS: *WiFi 6, cybersecurity, WPA3*

ანოტაცია: Wi-Fi 6, იგივე IEEE 802.11ax, წარმოადგენს უახლეს სტანდარტს უსადენო კავშირის ტექნოლოგიებში, რომელიც შემუშავებულია მზარდი ციფრული მოთხოვნების საპასუხოდ — განსაკუთრებით ისეთ სცენარებში, სადაც მრავალმოწყობილობრივი კავშირი საჭიროებს რესურსების ეფექტიან მართვას. აღნიშნული სტანდარტი არ შემოიფარგლება მხოლოდ გადაცემის სიჩქარისა და ქსელური გამტარობის გაუმჯობესებით; იგი აერთიანებს მოწინავე უსაფრთხოების მექანიზმებს, როგორიცაა WPA3 (Wi-Fi Protected Access 3), SAE (Simultaneous Authentication of Equals) და PMF (Protected Management Frames), რომლებიც მიზნად ისახავენ წინა ვერსიებში გამოვლენილი სისუსტეების აღმოფხვრას. წინამდებარე ნაშრომის მიზანია Wi-Fi 6 ტექნოლოგიის უსაფრთხოების ანალიზი, თანამედროვე კიბერსაფრთხეებზე რეაგირების მექანიზმების შეფასება და იმ ტექნიკური შესაძლებლობების გამოყოფა, რომლებიც განაპირობებენ აღნიშნული სტანდარტის ადაპტირებულობას დღევანდელ კიბერუსაფრთხოების გამოწვევებთან მიმართებაში.

საკვანძო სიტყვები: *WiFi 6, კიბერ უსაპრთხოება, WPA3*

1.შესავალი

დღევანდელ ციფრულ სამყაროში, სადაც ინტერნეტზე დამოკიდებულება დღითიდღე იზრდება და ერთ სივრცეში უამრავი მოწყობილობაა დაკავშირებული, უძლიერესი და ეფექტიანი უკაბელო კავშირის საჭიროება სულ უფრო მომწიფდება. Wi-Fi 6, ანუ IEEE 802.11ax, სწორედ ამ საჭიროებაზე პასუხია — ეს ახალი ტექნოლოგია გვთავაზობს უფრო სწრაფ და სტაბილურ კავშირს, რომელიც კარგად მუშაობს ისეთ „ცხელ“ და დატვირთულ ადგილებში, სადაც მრავალი მოწყობილობა ერთად მუშაობს. თუმცა, სიჩქარეზე და კომფორტზე მეტი, დღეს მთავარი თემა უსაფრთხოებაა. ინტერნეტზე მავნე თავდასხმები სულ უფრო რთულდება და ამიტომ Wi-Fi 6-ის შემქმნელებმა მნიშვნელოვანი უსაფრთხოების გაუმჯობესებები შეიტანეს — WPA3, SAE და სხვა მექანიზმების სახით.
ამ სტატიის მიზანია იმის გამოკვლევა თუ რამდენად უსაფრთხოა Wi-Fi 6 რეალურად, რა საფრთხეები ემუქრება მას დღეს და როგორ იცავს ის ჩვენს მონაცემებს. ეს კვლევა არ არის მხოლოდ ტექნიკური განმარტება — ეს მცდელობაა გავიგოთ, რამდენად მომზადებულია Wi-Fi 6 თანამედროვე კიბერუსაფრთხოების გამოწვევებისთვის და რა ნაბიჯები შეიძლება გადავდგათ უკეთესი დაცვისთვის.

2.Wi-Fi 6-ის ტექნიკური სპეციფიკაციები

Wi-Fi 6, იგივე IEEE 802.11ax, წარმოადგენს უახლეს სტანდარტს უსადენო ქსელებში, რომელიც შემუშავებულია არსებული ტექნოლოგიური გამოწვევების დასაძლევად. ის აერთიანებს მრავალ მნიშვნელოვან გაუმჯობესებას, რაც Wi-Fi 5-ის შესაძლებლობებს საგრძნობლად აჭარბებს. ერთ-ერთი მთავარი სიახლეა OFDMA (Orthogonal Frequency Division Multiple Access) ტექნოლოგია, რომელიც არხებს ყოფს მცირე რესურსულ ბლოკებად და შესაძლებელს ხდის მრავალ მოწყობილობას ერთდროულად ეფექტურად იმუშაოს. ამას ემატება MU-MIMO (Multi-User, Multiple Input, Multiple Output), რომელიც აწვდის მონაცემებს სხვადასხვა მომხმარებელს ერთდროულად და არა მორიგეობით, როგორც ადრე.
BSS Coloring ტექნოლოგია Wi-Fi 6-ს აძლევს უნარს, განსხვავება გააკეთოს მეზობელი ქსელების სიგნალებს შორის და შეამციროს ჩარევა. Target Wake Time (TWT) კი ხელს უწყობს ენერგიის დაზოგვას, რადგან მოწყობილობას საშუალებას აძლევს წინასწარ განსაზღვროს, როდის უნდა "გაიღვიძოს" და როდის იყოს არაქტიური. ასევე, 1024-QAM მოდულაციის გამოყენება მნიშვნელოვნად ზრდის მონაცემთა გადაცემის სიჩქარეს — დაახლოებით 25%-ით უფრო სწრაფია Wi-Fi 5-ის მიმართ. ამ ინოვაციებს ემატება ტექნოლოგიები, რომლებიც საერთო ჯამში ქმნიან უფრო სწრაფ, სტაბილურ და ეფექტურ კავშირს. მომხმარებლები იღებენ სარგებელს ისეთი მახასიათებლებით, როგორიცაა მაღალი სიჩქარე, დაბალი დაგვიანება (ლატენტობა), ენერგოეფექტურობა და გაუმჯობესებული შესრულება გადატვირთულ გარემოებში. ეს Wi-Fi 6-ს აქცევს განსაკუთრებით საჭირო ტექნოლოგიად სმარტ სახლებისთვის, ოფისებისთვის, უნივერსიტეტებისთვის, ვიდეოთამაშებისა და ვიდეო ზარებისთვის.
მთლიანობაში, Wi-Fi 6 წარმოადგენს მნიშვნელოვან წინგადადგმულ ნაბიჯს უსადენო ქსელების განვითარებაში. ის პასუხობს როგორც ინდივიდუალური მომხმარებლების მოთხოვნებს, ისე უფრო ფართო ინდუსტრიულ საჭიროებებს — მიანიჭოს სისტემებს უკეთესი სიჩქარე, ეფექტიანობა და, რაც მთავარია, მზარდი რაოდენობის მოწყობილობების მხარდაჭერა ერთი სივრციდან.

3.უსაფრთხოების მექნიზმები - WPA3, SAE, PMW

Wi-Fi 6-ს ხშირად განიხილავენ როგორც ტექნოლოგიას, რომელიც ინტერნეტის სიჩქარესა და სტაბილურობას აუმჯობესებს, მაგრამ რეალურად ის ბევრად უფრო მეტია, ვიდრე უბრალოდ სწრაფი კავშირი. ამ სტანდარტმა მნიშვნელოვანი ნაბიჯი გადადგა უსაფრთხოების მიმართულებითაც, რაც თანამედროვე ციფრულ სამყაროში უმნიშვნელოვანესია. წინა სტანდარტებთან შედარებით Wi-Fi 6-ში შეტანილია ისეთი მექანიზმები, რომლებიც ცდილობენ თავიდან აიცილონ როგორც ძველი, ისე ახალი ტიპის კიბერსაფრთხეები. ერთ-ერთი მთავარი სიახლეა WPA3 — დაცვის ახალი პროტოკოლი, რომელიც WPA2-ის შეცვლას ისახავს მიზნად. WPA2-ს ჰქონდა ცნობილი სისუსტეები, მათ შორის ცნობილი KRACK Attack, რომელიც საშუალებას აძლევდა თავდამსხმელს გაეშიფრა მონაცემები დაშიფრული კავშირიდან. WPA3 კი ამ ხარვეზებს აკორექტირებს და დამატებით იცავს მომხმარებელს ისეთი შეტევებისგან, როგორიცაა პაროლის გამოცნობის მცდელობები. WPA3-ის ნაწილი გახდა ახალი ავთენტიკაციის მექანიზმი, რომელსაც SAE (Simultaneous Authentication of Equals) ჰქვია. მისი მთავარი უპირატესობა ის არის, რომ პაროლი აღარ გადადის ქსელში არც დაუშიფრავად და არც მარტივად გამოსაცნობ ფორმაში. სისტემას შეუძლია გაარჩიოს, როდესაც თავდამსხმელი პაროლის გამოცნობას ცდილობს და თავიდანვე დაბლოკოს ასეთი ქცევა. Wi-Fi 6-ის კიდევ ერთი დაცვითი მექანიზმია PMF (Protected Management Frames), რომელიც იცავს ისეთ მონაცემებს, რომლებიც პასუხისმგებელია ქსელში მოწყობილობების დაკავშირებასა და მართვაზე. წარსულში ამ მონაცემებზე ხელმისაწვდომობა შესაძლებელი იყო, რაც ხშირად გამოიყენებოდა მომხმარებლის ქსელიდან "გადაგდებისთვის" ან ყალბი ქსელების შესაქმნელად. PMF ამას აბრკოლებს და ქსელის სტაბილურობას ზრდის. გარდა ამისა, ღია ქსელებისთვის Wi-Fi 6 გვთავაზობს OWE (Opportunistic Wireless Encryption) სისტემას, რომელიც დაშიფვრას იყენებს მაშინაც კი, როცა მომხმარებელი პაროლს საერთოდ არ შეიყვანს. ეს ნიშნავს, რომ კაფეში, ბიბლიოთეკაში ან საზოგადოებრივ ტრანსპორტში დაკავშირებულ მომხმარებლებსაც კი გარკვეული დონით დაცვა ექნებათ ერთმანეთისგან.
ყველა ეს მექანიზმი — WPA3, SAE, PMF და OWE — Wi-Fi 6-ს აქცევს არა მხოლოდ სწრაფ, არამედ ბევრად უფრო დაცულ ტექნოლოგიად, რომელიც უკვე რეალურად ებრძვის იმ საფრთხეებს, რომლებიც წინა სტანდარტებს ჰქონდა.

4.დღევანდელი კიბერსაფრთხეები Wi-Fi 6-ის პირობებში

Wi-Fi 6 დიდი ნაბიჯია წინ უსადენო ქსელების განვითარებაში — ის გვპირდება უფრო სწრაფ და სტაბილურ ინტერნეტს, უკეთეს მრავალმოწყობილობის მხარდაჭერას და ენერგიის დაზოგვას. მაგრამ, როგორც ხშირად ხდება ტექნოლოგიებში, სადაც მეტი კომფორტია, იქვე იმალება ახალი საფრთხეებიც. ამ ახალ სტანდარტს ახლავს თან უსაფრთხოების გაუმჯობესებული მექანიზმები, თუმცა არც ისინი არიან სრულიად დაუცველნი.
Wi-Fi 6-ში უსაფრთხოების მთავარი ბურჯია WPA3 — თანამედროვე დაშიფვრის პროტოკოლი, რომელიც ძველი WPA2-ის ნაკლოვანებების გასწორებას ისახავს მიზნად. WPA3-ს იყენებს ისეთი ფუნქციები, როგორებიცაა SAE (Simultaneous Authentication of Equals) და Protected Management Frames (PMF). ამ პროტოკოლებს შეუძლიათ დაცვა ისეთ შეტევებისგან, როგორიცაა პაროლების გამოცნობის მცდელობები ან დაუცველი ქსელების გამოყენება მომხმარებლის მონაცემების მოსაპარად. მაგალითად, WPA3-ში დაშიფვრა ყოველთვის ჩართულია და პაროლი აღარ გადადის დაუცველად. გარდა ამისა, გამოიყენება ე.წ.

forward secrecy — რაც ნიშნავს, რომ კავშირის დაშიფვრა ყოველ ჯერზე განსხვავებულია, და თუ ვინმემ ერთჯერადი მონაცემი მოიპოვა, წარსულის ან მომავლის კომუნიკაციას მაინც ვერ წაიკითხავს. თუმცა რეალობა ყოველთვის იდეალური არ არის. WPA3-ის დაცვის მიუხედავად, მკვლევრებმა დააფიქსირეს მისი სისუსტეებიც. ერთ-ერთი გავრცელებული საფრთხეა downgrade attack — თავდამსხმელი ცდილობს მოწყობილობა დააბრუნოს ძველ WPA2 პროტოკოლზე, სადაც გატეხვა გაცილებით მარტივია. ასევე არსებობენ გვერდითი არხის შეტევები, რომლებიც არ იყენებენ ჩვეულებრივ ქსელურ ხრიკებს, არამედ აპარატურის ან პროგრამული რეაქციების მეშვეობით ცდილობენ ინფორმაციაზე წვდომას. მნიშვნელოვანი საფრთხე მოდის IoT მოწყობილობებიდანაც. მიუხედავად იმისა, რომ Wi-Fi 6 მათ უკეთეს კავშირს სთავაზობს, მრავალი ასეთი მოწყობილობა მაინც არ ახორციელებს WPA3-ის სრულ მხარდაჭერას. ისინი ხშირად გამოირჩევიან დაბალი ხარისხის firmware-ით, არ მიიღებენ დროულ უსაფრთხოების განახლებებს და არ აქვს მკაცრი კონფიგურაციები. ეს კი მათ ჰაქერული შეტევებისთვის იდეალურ სამიზნედ აქცევს. საფრთხეს წარმოადგენს ადამიანური ფაქტორიც — WPA3 და Wi-Fi 6-ის ფუნქციები ხშირად არასწორად არის კონფიგურირებული ან საერთოდ გამორთული რჩება. ადმინისტრატორების დაუდევრობა ან ინფორმაციის ნაკლებობა ქმნის სივრცეს, სადაც ყველაზე თანამედროვე დაცვაც კი ვერ გვიცავს სრულად.

ამრიგად, Wi-Fi 6-ის მიღება ნამდვილად პროგრესია, მაგრამ უსაფრთხოების თვალსაზრისით ეს მხოლოდ საწყისი ეტაპია. იმისათვის, რომ ტექნოლოგიამ რეალურად მოგვანიჭოს დაცულობის შეგრძნება, საჭიროა სწორად კონფიგურირებული ინფრასტრუქტურა, განახლებების დროული ჩართვა და მუდმივი სიფხიზლე — რადგან საფრთხეები ყოველთვის ერთი ნაბიჯით ახლოს არიან.

5.როგორ ებრძვის Wi-Fi 6 არსებულ საფრთხეებს

Wi-Fi 6-ის სტანდარტი დღეს უკვე ბევრად მეტია, ვიდრე უბრალოდ ინტერნეტის სიჩქარის გაუმჯობესება — მისი ერთ-ერთი მთავარი მიღწევა უსაფრთხოების სფეროშია. წინა თაობების დროს მომხმარებლები ხშირად ექცეოდნენ სხვადასხვა კიბერსაფრთხის ქვეშ, დაწყებული პაროლის მოპარვით და დამთავრებული ღია Wi-Fi ქსელებზე ჩასაფრებული ჰაკერებით. Wi-Fi 6 კი ამ რეალურ საფრთხეებს პირდაპირ პასუხობს კონკრეტული მექანიზმებით. ერთ-ერთი ყველაზე მნიშვნელოვანი სიახლე არის WPA3, რაც WPA2-ის გაუმჯობესებული და ბევრად უფრო დაცული ვერსიაა. ამ სტანდარტში დაცულია პაროლის გადაცემის პროცესი — განსხვავებით ძველი მეთოდებისგან, სადაც პაროლი შეიძლებოდა ჩაჭრილიყო ან brute-force მეთოდით გატეხილიყო. Wi-Fi 6 იყენებს SAE (Simultaneous Authentication of Equals) პროტოკოლს, რომელიც ქმნის უნიკალურ დაშიფრულ კავშირს ყოველ ახალ შეერთებაზე. ეს ნიშნავს, რომ ვეღარავინ ჩაწერს handshake-ს და ვერ დაიწყებს ოფლაინ შეტევებს პაროლის გასატეხად — ყოველ ჯერზე ინფორმაცია ახალი გასაღებით შიფრირდება. მომხმარებელთა დაცვა მარტო პაროლით არ სრულდება. Wi-Fi 6-ში მოხვდა PMF (Protected Management Frames) მექანიზმი, რომელიც იცავს მოწყობილობებს ისეთ შეტევებისგან, რომლებიც ადრე თითქმის შეუმჩნეველი იყო. მაგალითად, როცა ჰაკერი აგზავნიდა “deauthentication” სიგნალს და გაწყვეტინებდა მომხმარებელს ინტერნეტს, ახლა უკვე მართვის ყველა კადრი დაშიფრულია, რაც კავშირების სტაბილურობასაც იცავს და დაუფარავ შეტევებსაც აფერხებს. Wi-Fi 6-ს აქვს კიდევ ერთი პრაქტიკული დაცვითი საშუალება — OWE (Opportunistic Wireless Encryption), რომელიც განსაკუთრებით მნიშვნელოვანია საზოგადოებრივი Wi-Fi-ს გამოყენებისას. ადრე

ღია ქსელებში, როგორიცაა კაფეები ან აეროპორტები, მომხმარებლის მონაცემები დაუცველად გადაიცემოდა. Wi-Fi 6 კი თითო მომხმარებლის კავშირს ინდივიდუალურად შიფრავს, რაც იმას ნიშნავს, რომ ჰაკერს, რომელსაც სურს გაიგოს რას წერ Messenger-ში ან რომელ საიტებზე შედიხარ, ეს პრაქტიკულად აღარ გამოუვა. გარდა ამისა, Wi-Fi 6 Enterprise რეჟიმში იყენებს 192-ბიტიან დაშიფვრას და ძლიერ ავთენტიკაციის მექანიზმებს, რაც განსაკუთრებით მნიშვნელოვანია კომპანიებისთვის. ეს მექანიზმები არა მხოლოდ გარე საფრთხეებს, არამედ შიდა ინფორმაციულ დარღვევებსაც ამცირებს და მეტად აკონტროლებს ქსელზე წვდომას.
საბოლოოდ, Wi-Fi 6-ის უსაფრთხოების მექანიზმები სწორედ რეალურ, ყოველდღიურ საფრთხეებზეა მორგებული — და სწორედ ეს ხდის მას სანდო სტანდარტად ციფრულ ეპოქაში. იგი აღარ გვთავაზობს უბრალოდ კავშირს, არამედ აშენებს დაცულ და ჭკვიან ეკოსისტემას, რომელიც მუდმივად იცავს მომხმარებლის მონაცემებს თანამედროვე კიბერსაფრთხეების ფონზე.

დადასტურება

აღნიშნული ნაშრომი შესრულებულია შოთა რუსთაველის საქართველოს ეროვნული სამეცნიერო ფონდის მხარდაჭერით - SPG-24-307.

ბიბლიოგრაფია

1. Wikipedia. (n.d.). *IEEE 802.11ax*. Retrieved June 17, 2025, from https://en.wikipedia.org/wiki/IEEE_802.11ax
2. Intel Corporation. (n.d.). *Wi-Fi 6: Faster, Smarter and More Secure*. Retrieved June 17, 2025, from https://www.intel.com/content/www/us/en/architecture-and-technology/wifi-6.html
3. Cisco Meraki. (2018, June). *Wi-Fi 6: The Next Generation of Wireless*. Retrieved June 17, 2025, from https://meraki.cisco.com/blog/2018/06/wi-fi-6-the-next-generation-of-wireless/
4. NXP Semiconductors. (n.d.). *Understanding Wi-Fi 6*. Retrieved June 17, 2025, from https://www.nxp.com/wifi6
5. Network World. (n.d.). *What is Wi-Fi 6?*. Retrieved June 17, 2025, from https://www.networkworld.com/article/3328987/what-is-wi-fi-6.html
6. Wi-Fi Alliance. (n.d.). *WPA3 Overview & Technical Resources*. Retrieved June 17, 2025, from https://www.wi-fi.org/discover-wi-fi/security
7. Cisco Systems. (n.d.). *Understanding Wi-Fi 6 Security*. Retrieved June 17, 2025, from https://www.cisco.com
8. IEEE Standards Association. (2021). *IEEE 802.11ax Standard Documentation*. Retrieved June 17, 2025, from https://standards.ieee.org/standard/802_11ax-2021.html
9. TechTarget. (n.d.). *WPA3: Benefits and Challenges in Wireless Security*. Retrieved June 17, 2025, from https://www.techtarget.com/searchsecurity/definition/WPA3
10. Ars Technica. (n.d.). *WPA3 Security Analysis and Limitations*. Retrieved June 17, 2025, from https://arstechnica.com/information-technology/