Раздел 3. «Информационно-коммуникационные технологии»

ҒТАМР 28.23.15
ӘОЖ 004.056.5

DOI: 10.53002/076

Э.В. Харин

Карагандинский индустриальный университет, г. Темиртау
(E-mail: e.kharin@tttu.edu.kz)

MAC қауіпсіздігіндегі протоколдары және оның желілік қауіпсіздігіндегі рөлі

Media Access Control (MAC) деңгейі желілік байланыстың маңызды құрамдас бөлігі болып табылады, ол құрылғылардың ортақ орта арқылы деректерге қол жеткізу және беру жолын басқаруға жауап береді. Бұл құжат қауіпсіздік мәселелерін шешу кезінде деректерді тиімді тасымалдауды жеңілдететін Ethernet және Wi-Fi сияқты негізгі MAC деңгей протоколдарын зерттейді. Әртүрлі сенім механизмдерімен, соның ішінде аутентификация хаттамалары мен қауіпсіздікті арттыратын шифрлау әдістерімен қатар MAC деңгейінің осалдықтары, мысалы, MAC спуфинг және VLAN секіру талқыланады. Бұл тетіктерді енгізу MAC деңгейінің осалдықтарымен байланысты тәуекелдерді айтарлықтай азайтып, желі қауіпсіздігі мен жалпы тұтастығын күшейтуге ықпал етеді.

Түйін сөздер: MAC деңгейі, желілік қауіпсіздік, Ethernet, Wi-Fi, MAC спуфинг, VLAN секіру, сенім механизмдері, аутентификация протоколдары, шифрлау, MACsec, желінің осалдықтары.

Кіріспе

Media Access Control (MAC) деңгейі OSI моделінің негізгі құрамдас бөлігі болып табылады, ол желідегі құрылғылардың байланыс ортасына қатынасу жолын басқаруға жауапты екінші деңгей ретінде қызмет етеді. Ол маңызды желілік хаттамаларды басқару арқылы деректерді тиімді тасымалдауды қамтамасыз етуде шешуші рөл атқарады. Мысалы, Ethernet сымды желілер арқылы деректерді жіберуді басқару үшін Carrier Sense Multiple Access with Collision Detection (CSMA/CD) пайдаланады, ал Wi-Fi сымсыз байланыс үшін Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) пайдаланады. Бұл хаттамалар деректердің соқтығысуын болдырмау және желіге кіруді басқару арқылы желінің тиімділігі мен сенімділігін қолдау үшін өте маңызды [5, б. 8–9].

MAC деңгейіндегі қауіпсіздік мәселелері.

MAC деңгейі ең алдымен өзіне тән осалдықтарына байланысты күрделі қауіпсіздік мәселелеріне тап болады. Бұл қиындықтар желілік байланыс хаттамаларының іргелі дизайнынан және заманауи желілік инфрақұрылымдардың күрделене түсуінен туындайды.

MAC жалғандығы зиянкестер өздерінің құрылғыларының MAC мекенжайын өзгертіп, рұқсатсыз желіге қол жеткізе отырып, заңды құрылғылардың кейпіне енетін маңызды қауіп болып табылады. Бұл әдіс көптеген желілік қауіпсіздік механизмдерінің сенімге негізделген сипатын пайдаланады. Сенімді құрылғының MAC мекенжайын имитациялау арқылы зиянды әрекетшілер дәстүрлі кіруді басқару элементтерін айналып өтіп, шектеулі желі сегменттеріне кіруге немесе сезімтал байланыстарды ұстауға мүмкіндік алады [12, б. 3].

VLAN Hopping – шабуылдаушыларға желі трафигін сегменттеуге арналған қауіпсіздік шараларын айналып өтіп, пакеттерді әртүрлі VLAN желілеріне жіберуге мүмкіндік беретін жетілдірілген шабуыл әдісі. Әдетте, VLAN секіру екі негізгі әдіс арқылы жүзеге асады: ауыстырып-қосқыш спуфинг және қос тегтеу. Коммутатордың спуфингінде шабуылдаушылар өздерінің желілік интерфейсін магистральдық режимге конфигурациялайды, мүмкін бірнеше VLAN желісіне қол жеткізе алады. Қос таңбалау желіні оқшаулау принциптерін тиімді айналып өтіп, VLAN шекараларын кесіп өтетін арнайы жобаланған желі пакеттерін жасауды қамтиды [7].

Раздел 3. «Информационно-коммуникационные технологии»

Осы арнайы шабуыл векторларынан басқа, MAC деңгейі қауіпсіздік мәселелерінің кең спектріне қарсы тұрады. РЖ кептелу шабуылдары, әсіресе сымсыз желілерде маңызды қауіп болып табылады. Бұл шабуылдар сымсыз байланыс жиіліктеріне әдейі кедергі жасауды, желі қосылымын әлеуетті бұзуды немесе күрделі енулер үшін осалдықтарды жасауды қамтиды [1, б. 1].

Man-in-the-Middle (MitM) шабуылдары MAC деңгейінде де маңызды алаңдаушылық тудырады. Осы іргелі деңгейде желілік трафикті ұстау және ықтимал манипуляциялау арқылы шабуылдаушылар коммуникацияларды тыңдай алады, зиянды мазмұнды енгізе алады немесе бұзылған соңғы нүктелер арқылы желілік трафикті қайта бағыттай алады [2].

Address Resolution Protocol (ARP) кэшті улану тағы бір күрделі шабуыл әдісін ұсынады. Жалған ARP хабарламаларын жіберу арқылы шабуылдаушылар өздерінің MAC мекенжайын заңды IP мекенжайларымен байланыстыра алады, бұл оларға желілік байланыстарды ұстап тұруға және трафикті өз құрылғылары арқылы ықтимал қайта бағыттауға мүмкіндік береді [11].

Осы MAC деңгейінің қауіпсіздік мәселелерінен қорғау көп деңгейлі тәсілді қажет етеді. Желі әкімшілері қатаң MAC мекенжайын сүзгілеуді енгізу, 802.1X аутентификация механизмдерін пайдалану, динамикалық ARP тексеруін конфигурациялау, желі коммутаторларындағы порт қауіпсіздік мүмкіндіктерін пайдалану, желілік инфрақұрылым микробағдарламасын жүйелі түрде жаңарту және кешенді желі мониторингі мен аномалияларды анықтау жүйелерін енгізу сияқты сенімді қауіпсіздік шараларын орындауы керек.

Желілік технологиялар дамып келе жатқандықтан, MAC деңгейінің қауіпсіздігі өздерінің цифрлық инфрақұрылымын барған сайын күрделі киберқауіптерден қорғауға ұмтылатын ұйымдар үшін маңызды мәселе болып қала береді.

Методология. MAC деңгейі құрылғылардың желілік ортаға кіру жолын басқару үшін өте маңызды. Дегенмен, ол желі қауіпсіздігі мен өнімділігіне әсер ететін шабуылдаушылар пайдаланатын әртүрлі осалдықтарға бейім. Бұл бөлім Ethernet, Wi-Fi, Zigbee және Bluetooth [3] сияқты MAC деңгейлерінің әртүрлі протоколдарындағы осы осалдықтарды зерттейді.

Жалпы осалдықтар. Ethernet маңызды қауіпсіздік мәселелерін ұсынады. MAC Spoofing шабуылдаушыларға рұқсат етілмеген кіруге ие болып, заңды құрылғылардың атын шығару үшін өздерінің MAC мекенжайларын өзгертуге мүмкіндік береді. VLAN Hopping — зиянды әрекетшілер VLAN конфигурацияларын тиісті рұқсатсыз VLAN желілері арасында пакеттерді жіберу үшін пайдаланатын тағы бір маңызды осалдық [4].

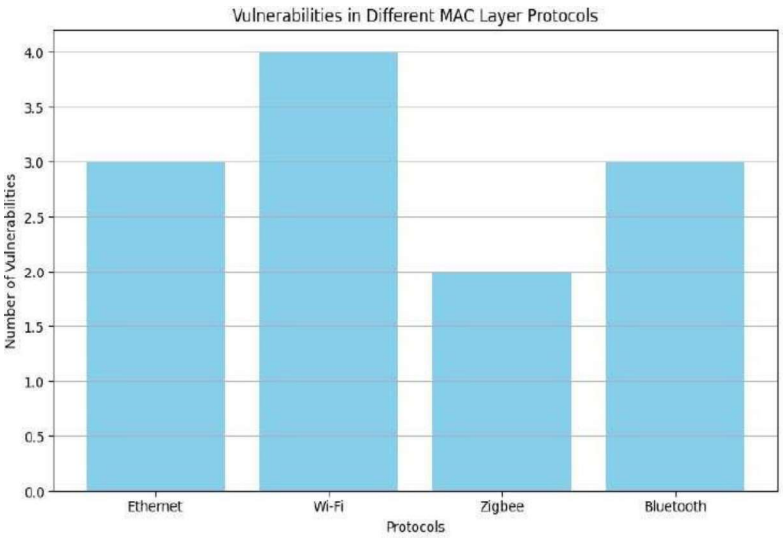
Wi-Fi желілері әртүрлі қауіптерге, соның ішінде жалған аутентификация кадрларын жіберу арқылы құрылғыларды ажыратуға мәжбүрлейтін аутентификация шабуылдарына тап болады. Қауіпсіздік конфигурацияларының әлсіздігіне байланысты шабуылдаушылар шифрланбаған деректерді ұстай отырып, тыңдау тұрақты қауіп болып қала береді [4].

Zigb протоколдары кілттерді басқару ақауларына осал, мұнда шифрлау кілттерін қауіпсіз сақтау және беру рұқсатсыз кіруге әкелуі мүмкін. Желінің кептелуі тағы бір маңызды қауіп төндіреді, шабуылдаушылар желіге кедергі келтіріп, байланысты бұзады [6].

Bluetooth технологиясы қауіпсіздік қауіптеріне қарсы емес. Bluejacking Bluetooth қосылған құрылғыларға қажетсіз хабарларды жіберуге мүмкіндік береді, ал Bluesnarfing Bluetooth құрылғыларында сақталған ақпаратқа рұқсатсыз кіруге мүмкіндік береді [3].

Бұл осалдықтар ықтимал бұзушылықтар мен рұқсатсыз кіруден қорғау үшін сенімді қауіпсіздік шаралары мен әртүрлі желілік протоколдар арқылы үздіксіз бақылаудың маңызды қажеттілігін көрсетеді.

Раздел 3. «Информационно-коммуникационные технологии»



Сурет 1. Әртүрлі MAC деңгей хаттамаларындағы осалдықтар.

Бұл 1-сурет MAC деңгейінің әртүрлі протоколдарымен байланысты осалдықтардың санын көрсетеді:

• Wi-Fi осалдықтардың ең көп санын көрсетеді, бұл ең алдымен оның кеңінен таралуына және аутентификация шабуылдары мен тыңдау сияқты ішкі қауіпсіздік мәселелеріне байланысты.

• Ethernet пен Bluetooth жиі спуфингке және деректерге рұқсатсыз кіруге қатысты орташа осалдық деңгейлеріне ие.

• Zigbee аз қуатты IoT қолданбаларына арналған болса да, кілттерді басқару және желіні кептелумен байланысты қиындықтарға тап болады.

Осалдықтардың салдары. MAC деңгейінің осалдықтарының болуы желі қауіпсіздігі мен операциялық тұтастық үшін терең және ауқымды салдарларға әкелуі мүмкін. Мәліметтерді бұзу ең маңызды тәуекелдердің бірі болып табылады, мұнда құпия ақпаратқа рұқсатсыз қол жеткізу ұйымдық құпиялылыққа нұқсан келтіруі мүмкін, маңызды іскерлік, жеке немесе қаржылық деректерді зиянды әрекеттерге жіберуі мүмкін [12, б. 5].

Желідегі үзілістер тағы бір маңызды қиындық тудырады. Кептелу сияқты шабуылдар бүкіл желілік инфрақұрылымдарды уақытша немесе тұрақты түрде жарамсыз етіп, айтарлықтай жұмыс уақытын және ықтимал экономикалық шығындарды тудыруы мүмкін. Бұл үзілістер үздіксіз желі қосылымына қатты сенетін ұйымдар үшін әсіресе жойқын болуы мүмкін [1, б. 4-5].

Ресурстардың сарқылуы тұрақты желілік шабуылдардың нәзік, бірақ әсерлі салдары ретінде пайда болады. Үздіксіз зиянды әрекеттер құрылғы ресурстарын құртуы мүмкін, жалпы желі өнімділігіне айтарлықтай әсер етеді, жүйенің тиімділігін төмендетеді және аппараттық құралдың мерзімінен бұрын нашарлауына әкелуі мүмкін [13, б. 6].

Әсер ету стратегиялары.

Бұл осалдықтарды жою желі қауіпсіздігіне кешенді және белсенді көзқарасты талап етеді. Күшті аутентификация механизмдерін енгізу қорғаныстың маңызды бірінші желісі болып табылады. Күшті аутентификация хаттамалары рұқсатсыз кіру қаупін және желіге ықтимал ену қаупін айтарлықтай төмендете отырып, құрылғы идентификациясын тиімді тексере алады [13, б. 7].

Жетілдірілген шифрлау әдістері, әсіресе AES сияқты стандарттарды қолдану деректердің тұтастығы мен құпиялылығын қорғауда шешуші рөл атқарады. Желілік коммуникацияларды шифрлау арқылы ұйымдар ұсталған деректерді ықтимал шабуылдаушылар үшін іс жүзінде оқылмайтын ететін қауіпсіздіктің қосымша деңгейін жасай алады [9, б. 5].

Тұрақты қауіпсіздік аудитін жүргізу тағы бір маңызды стратегияны білдіреді. Бұл жүйелі бағалаулар ұйымдарға желіні қорғау механизмдерін үздіксіз жетілдіруді қамтамасыз ете отырып, әлеуетті қауіпсіздік олқылықтарын пайдаланбас бұрын анықтауға және түзетуге көмектеседі.

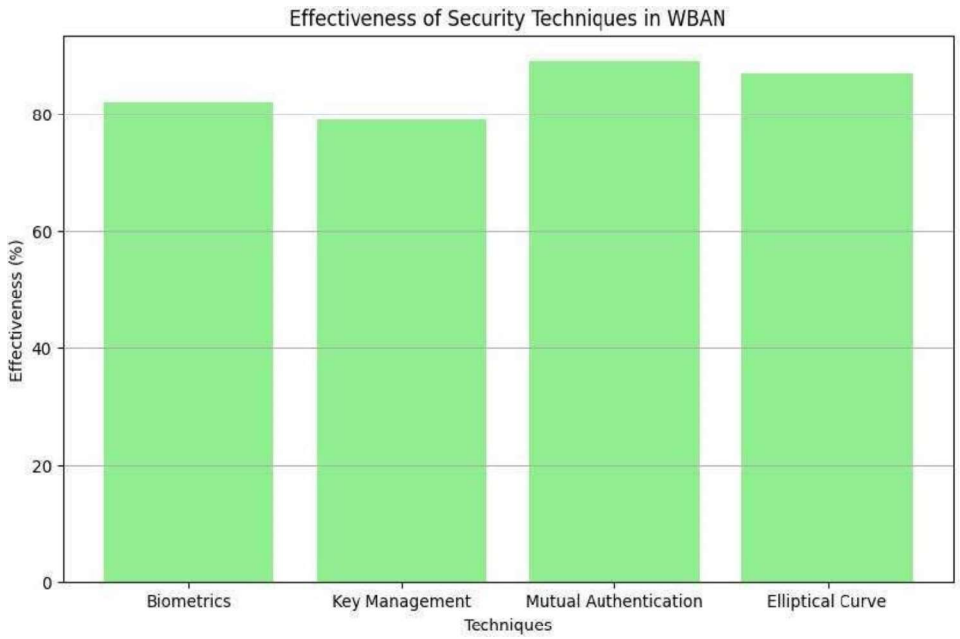
Осы осалдықтарды түсіну және жою арқылы ұйымдар барлық құрылғыларда сенімді және қауіпсіз байланысты қамтамасыз ете отырып, өз желілерінің қауіпсіздігін арттыра алады. Бұл тәсіл желі

қауіпсіздігін реактивті шарадан жалпы ұйымдық тәуекелдерді басқарудың белсенді, стратегиялық құрамдас бөлігіне айналдырады.

Зерттеу нәтижелері. MAC деңгейіндегі осалдықтарды жою үшін қауіпсіздікті арттыру және желіні сенімді қорғауды қамтамасыз ету үшін әртүрлі сенім механизмдері енгізілді. Бұл механизмдер аутентификацияға, шифрлауға және желілік трафиктің тұтастығына бағытталған.

Аутентификация протоколдары желідегі құрылғылардың идентификациясын тексеруде маңызды рөл атқарады. Бұл хаттамалар желіге тек рұқсат етілген құрылғылардың қол жеткізуін қамтамасыз етеді, бұл MAC спуфингінен және басқа сәйкестікке негізделген шабуылдардан туындайтын қауіптерді азайтады. Мысалдар байланыс орнату алдында бір-бірін аутентификациялауды қажет ететін екі қатынасушы тараптың да сұрау-жауап механизмдерін және өзара аутентификацияны қамтиды. Мұндай хаттамалар құрылғы идентификациясының тұтастығы деректер қауіпсіздігіне тікелей әсер ететін сценарийлерде өте маңызды [10, б. 7].

Шифрлау әдістері деректердің тұтастығын және тасымалдау кезінде құпиялылықты қорғау арқылы қосымша қауіпсіздік деңгейін қамтамасыз етеді. Мысалы, MACsec (Media Access Control Security) - құрылғылар арасындағы трафикті шифрлау арқылы Ethernet қосылымдарын қорғауға арналған 2 деңгейлі шифрлау протоколы. Бұл шабуылдаушылар физикалық желіге қол жеткізген жағдайда да деректерді рұқсатсыз ұстауға жол бермейді [9, б. 3].



Сурет 2. WBAN жүйесіндегі қауіпсіздік техникасының тиімділігі.

2-суретте көрсетілгендей, эллиптикалық қисық криптография (ECC) сияқты шифрлау әдістері сымсыз дене аймағының желілері (WBANs) сияқты шектеулі ресурстары бар орталарда жоғары тиімді. Бұл әдістер күшті шифрлауды төмен есептеу шығындарымен біріктіреді, бұл оларды денсаулық сақтау және IoT қолданбалары үшін әсіресе қолайлы етеді.

Тиімділікті талдау. 2-суретте көрсетілгендей, қауіпсіздіктің әртүрлі әдістері әртүрлі тиімділік дәрежесін көрсетеді:

• Биометрия: пайдаланушы аутентификациясының күшті механизмін қамтамасыз етеді, бірақ биометриялық деректердің дәлдігіне байланысты.

• Кілтті басқару: шифрланған байланыс арналарын қолдау үшін маңызды болып табылатын криптографиялық кілттердің қауіпсіз таралуын және сақталуын қамтамасыз етеді.

• Өзара аутентификация: рұқсатсыз кіруді тиімді болдырмайтын байланыс процесінде екі соңғы нүктені де тексеру арқылы қауіпсіздіктің ең жоғары деңгейлерінің бірін ұсынады.

• Эллиптикалық қисық криптография (ECC): Күшті шифрлау мен төмен қуат тұтыну арасындағы тепе-теңдік арқасында ерекше тиімділікті көрсетеді, бұл оны WBAN және басқа ресурс шектеулі орталар үшін тамаша етеді.

Кейс зерттеулері. Нақты әлемдік енгізулер сенім механизмдерінің тиімділігін одан әрі көрсетеді:

• MACsec пайдаланатын желілер кәсіпорын деңгейіндегі орналастыруларда байқалғандай, MAC су тасқыны шабуылдарына және портты ұрлау оқиғаларына тиімді қарсы тұра алатыны көрсетілген.

• Денсаулық сақтау саласында өзара аутентификация хаттамалары және ECC бар WBANs пациент деректерін қауіпсіз тасымалдауды қамтамасыз етеді, ұстап алу немесе бұрмалау қаупін азайтады [8].

Осы сенім механизмдерін біріктіру арқылы желілер сенімді байланыс пен деректердің тұтастығын қамтамасыз ете отырып, бірқатар қауіпсіздік қатерлеріне қарсы тұрақтылығын айтарлықтай арттыра алады.

Қорытынды.

Media Access Control (MAC) деңгейі технологиялық әлеуетті де, қауіпсіздік мәселелерін де қамтитын желілік байланыстың маңызды түйінін білдіреді. Ethernet желісінен Wi-Fi-ға дейін әрбір протокол MAC спуфинг, VLAN өту және аутентификация шабуылдарын қоса, күрделі шабуылдаушылар пайдалана алатын бірегей осалдықтарды ұсынады. Бұл қауіптер осы іргелі қабаттағы желі қауіпсіздігінің күрделі көрінісін көрсетеді.

MAC деңгейін қамтамасыз ету тек техникалық талап емес, қазіргі заманғы ұйымдар үшін стратегиялық императив болып табылады. Тиімді жұмсарту сенімді аутентификация механизмдерін, кеңейтілген шифрлау әдістерін және қатаң қауіпсіздік аудиттерін біріктіретін көп қырлы тәсілді қажет етеді. Кешенді стратегияларды жүзеге асыру арқылы ұйымдар ықтимал осалдықтарды өздерінің желілік инфрақұрылымын нығайту мүмкіндіктеріне айналдыра алады.

Желілік технологиялар дамып келе жатқанда, MAC деңгейі киберқауіпсіздіктегі маңызды шайқас алаңы болып қала береді. Қауіпсіздігіне басымдық беретін ұйымдар құпия деректерді қорғауға, желінің тұтастығын сақтауға және цифрлық байланыстың барған сайын жетілдірілген ландшафтында шарлауға жақсырақ орналасады. Желілік қауіпсіздіктің болашағы дәлдікпен және тұрақтылықпен пайда болатын қауіптерді болжау, анықтау және оларға жауап беру ептілігін дамытуда жатыр.

Әдебиеттер тізімі

1. Ali, A. S., Baddeley, M., Bariah, L., Lopez, M. A., Lunardi, W. T., Giacalone, J., & Muhaidat, S. (2022). JAMRF: Performance analysis, evaluation, and implementation of RF jamming over Wi-Fi. I.E.E.E. Access, 10, 133370–133384. https://doi.org/10.1109/access.2022.3230895;

2. Al-Shareeda, M. A., Anbar, M., Manickam, S., & Hasbullah, I. H. (2020, July 29). Review of Prevention Schemes for Man-In-The-Middle (MITM) Attack in Vehicular Ad hoc Networks. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3662935;

3. Blancaflor, E., Purificacion, P. M. G., Atienza, R. B., Yao, J. J. M., & Alvarez, D. A.

C. (2023). Exploring the depths of Bluetooth attacks: A critical analysis of Bluetooth exploitation and awareness of users. Proceedings of the 2023 6th International Conference on Computing and Big Data (ICCBD), Shanghai, China, 52–59. https://doi.org/10.1109/ICCBD59843.2023.10607255;

4. Jiang, Z., Zhao, K., Li, R., Zhao, J., & Du, J. (2020). PHYAlert: Identity spoofing attack detection and prevention for a wireless edge network. Journal of Cloud Computing: Advances, Systems and Applications, 9(5). https://doi.org/10.1186/s13677-020-0154-7;

5. Kaur, M., Bajaj, R., & Kaur, N. (2021). A review of MAC layer for wireless body Area Network. Journal of Medical and Biological Engineering, 41(6), 767–804. https://doi.org/10.1007/s40846-021-00669-1;

6. Khanji, S., Iqbal, F., & Hung, P. (2019). ZigBsecurity vulnerabilities: Exploration and evaluating. 2019 10th International Conference on Information and Communication Systems (ICICS), 52-57. https://doi.org/10.1109/IACS.2019.8809115;

7. Kim, K., & Lee, M. (2018). SNMP-Based Detection of VLAN hopping attack Risk. In Lecture notes in electrical engineering (pp. 267–272). https://doi.org/10.1007/978-981- 13-1056-0_28;

8. Lackorzynski, T., Garten, G., Huster, J. S., Köpsell, S., & Hartig, H. (2020). Enabling and optimizing MACsec for industrial environments (Extended abstract). 2020 16th I.E.E.E. International Conference on Factory Communication Systems (WFCS), 1-4. https://doi.org/10.1109/WFCS47810.2020.9114434;

9. Oluyede, M. S., Mart, J., Olusola, A., & et al. (2024). The performance analysis of MACsec in different network environments. ScienceOpen Preprints. https://doi.org/10.14293/PR2199.000736.v1;

10. Preethichandra, D. M. G., Piyathilaka, L., Izhar, U., Samarasinghe, R., & De Silva,

L. C. (2023). Wireless body area networks and their applications—A review. I.E.E.E. Access, 11, 9202–9220. https://doi.org/10.1109/ACCESS.2023.3239008;

11. Prabadevi, B., Jeyanthi, N., & Abraham, A. (2019). An analysis of security solutions for ARP poisoning attacks and its effects on medical computing. International Journal of Systems Assurance Engineering and Management, 11(1), 1–14. https://doi.org/10.1007/s13198-019-00919-1;

12. Punia, S. K., & Ziya, F. (2019). Study on MAC protocols and attacks: A review. Proceedings of the 2019 6th International Conference on Computing for Sustainable Global Development (INDIACom),New Delhi, India, 621–625. https://doi.org/10.1109/INDIACom.2019.8745072;

13. Usman, M., Asghar, M. R., Ansari, I. S., & Qaraqe, M. (2018). Security in wireless body area networks: From in-body to off-body communications. I.E.E.E. Access, 6, 58064– 58074. https://doi.org/10.1109/ACCESS.2018.2873825

Э.В. Харин

Протоколы безопасности MAC и его роль в сетевой безопасности

Уровень Media Access Control (MAC) является важным компонентом сетевого взаимодействия, который отвечает за управление тем, как устройства получают доступ и передают данные через общую среду. В этом документе исследуются основные протоколы уровня MAC, такие как Ethernet и Wi-Fi, которые облегчают эффективную передачу данных при решении проблем безопасности. Наряду с различными механизмами доверия, включая протоколы аутентификации и методы шифрования, повышающие безопасность, обсуждаются уязвимости уровня MAC, такие как спуфинг MAC и переход VLAN. Внедрение этих механизмов значительно снизит риски, связанные с уязвимостями уровня MAC, и будет способствовать повышению сетевой безопасности и общей целостности.

Ключевые слова: уровень MAC, сетевая безопасность, Ethernet, Wi-Fi, спуфинг MAC, переход VLAN, механизмы доверия, протоколы аутентификации, шифрование, MACsec, сетевые уязвимости.

E.V. Kharin

Mac security protocols and its role in network security

The Media Access Control (MAC) layer is an important component of network communication, which is responsible for controlling the way devices access and transmit data through a shared environment. This document explores basic MAC layer protocols such as Ethernet and Wi-Fi, which make it easier to transfer data efficiently while addressing security issues. Along with various trust mechanisms, including authentication protocols and encryption methods that increase security, MAC-level vulnerabilities such as MAC spoofing and VLAN hopping are discussed. The implementation of these mechanisms will significantly reduce the risks associated

with MAC-level vulnerabilities and contribute to strengthening network security and overall integrity.

Keywords: MAC level, network security, Ethernet, Wi-Fi, MAC spoofing, VLAN jump, trust mechanisms, authentication protocols, encryption, MACsec, network vulnerabilities.

References

1. Ali, A. S., Baddeley, M., Bariah, L., Lopez, M. A., Lunardi, W. T., Giacalone, J., & Muhaidat, S. (2022). JAMRF: Performance analysis, evaluation, and implementation of RF jamming over Wi-Fi. I.E.E.E. Access, 10, 133370–133384. https://doi.org/10.1109/access.2022.3230895;

2. Al-Shareeda, M. A., Anbar, M., Manickam, S., & Hasbullah, I. H. (2020, July 29). Review of Prevention Schemes for Man-In-The-Middle (MITM) Attack in Vehicular Ad hoc Networks. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3662935;

3. Blancaflor, E., Purificacion, P. M. G., Atienza, R. B., Yao, J. J. M., & Alvarez, D. A.

C. (2023). Exploring the depths of Bluetooth attacks: A critical analysis of Bluetooth exploitation and awareness of users. Proceedings of the 2023 6th International Conference on Computing and Big Data (ICCBD), Shanghai, China, 52–59. https://doi.org/10.1109/ICCBD59843.2023.10607255;

4. Jiang, Z., Zhao, K., Li, R., Zhao, J., & Du, J. (2020). PHYAlert: Identity spoofing attack detection and prevention for a wireless edge network. Journal of Cloud Computing: Advances, Systems and Applications, 9(5). https://doi.org/10.1186/s13677-020-0154-7;

5. Kaur, M., Bajaj, R., & Kaur, N. (2021). A review of MAC layer for wireless body Area Network. Journal of Medical and Biological Engineering, 41(6), 767–804. https://doi.org/10.1007/s40846-021-00669-1;

6. Khanji, S., Iqbal, F., & Hung, P. (2019). ZigBsecurity vulnerabilities: Exploration and evaluating. 2019 10th International Conference on Information and Communication Systems (ICICS), 52-57. https://doi.org/10.1109/IACS.2019.8809115;

7. Kim, K., & Lee, M. (2018). SNMP-Based Detection of VLAN hopping attack Risk. In Lecture notes in electrical engineering (pp. 267–272). https://doi.org/10.1007/978-981- 13-1056-0_28;

8. Lackorzynski, T., Garten, G., Huster, J. S., Köpsell, S., & Hartig, H. (2020). Enabling and optimizing MACsec for industrial environments (Extended abstract). 2020 16th I.E.E.E. International Conference on Factory Communication Systems (WFCS), 1-4. https://doi.org/10.1109/WFCS47810.2020.9114434;

9. Oluyede, M. S., Mart, J., Olusola, A., & et al. (2024). The performance analysis of MACsec in different network environments. ScienceOpen Preprints. https://doi.org/10.14293/PR2199.000736.v1;

10. Preethichandra, D. M. G., Piyathilaka, L., Izhar, U., Samarasinghe, R., & De Silva,

L. C. (2023). Wireless body area networks and their applications—A review. I.E.E.E. Access, 11, 9202–9220. https://doi.org/10.1109/ACCESS.2023.3239008;

11. Prabadevi, B., Jeyanthi, N., & Abraham, A. (2019). An analysis of security solutions for ARP poisoning attacks and its effects on medical computing. International Journal of Systems Assurance Engineering and Management, 11(1), 1–14. https://doi.org/10.1007/s13198-019-00919-1;

12. Punia, S. K., & Ziya, F. (2019). Study on MAC protocols and attacks: A review. Proceedings of the 2019 6th International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, India, 621–625. https://doi.org/10.1109/INDIACom.2019.8745072;

13. Usman, M., Asghar, M. R., Ansari, I. S., & Qaraqe, M. (2018). Security in wireless body area networks: From in-body to off-body communications. I.E.E.E. Access, 6, 58064– 58074. https://doi.org/10.1109/ACCESS.2018.2873825