https://doi.org/10.53360/2788-7995-2025-1(17)-4

МРНТИ: 81.93.29

А.К. Шайханова[1,2*], Р.А. Буденов[2], О.Ш. Сатиев[2], Д.А. Тлепов [2], А.К. Токкулиева[1]
[1]Л.Н. Гумилев атындағы Еуразия ұлттық университеті,
Қазақстан Республикасы, Астана, Қ. Сәтпаев көшесі, 2,
[2]«WebTotem» ЖШС,
Қазақстан Республикасы, Астана, Қабанбай батыр даңғылы 51/1
[*]e-mail: aigul.shaikhanova@gmail.com

ҚАУІПСІЗ СМАРТФОНДЫ ЖОБАЛАУ ҮШІН WI-FI ЖӘНЕ LTE СЫМСЫЗ ЖЕЛІЛЕРІНІҢ ОСАЛДЫҒЫН ТАЛДАУ

Аңдатпа: *Бұл жұмыста қауіпсіз смартфонды жобалау контекстінде Wi-Fi сымсыз желілерінің (WEP, WPA, WPA2, WPA3) және LTE осалдықтарының практикалық талдау нәтижелерін ұсынады. Зерттеу Aircrack-ng, Wireshark, YateBTS және бағдарламалық қамтамасыз етумен анықталған BladeRF 2.0 радиосын қоса алғанда, құралдар кешенін пайдалана отырып жүргізілді, бұл шабуыл механизмдерін және заманауи хаттамалардың әртүрлі қауіп түрлеріне төзімділігін егжей-тегжейлі зерттеуге мүмкіндік берді.*

Эксперименттік бөлім енуді тестілеуге арналған стендтер мен автоматтандырылған сценарийлерді әзірлеуді қамтыды. Талдау WEP протоколының маңызды осалдықтары бар екенін және оны небәрі 4 секундта бұзуға болатынын көрсетті. WPA2 аутентификация пакеттерін ұстауға байланысты шабуылдарға ұшырады, бұл ортадағы адам (MITM) шабуылдарын жүзеге асыруға мүмкіндік береді. Жақсартуларға қарамастан, WPA3 сонымен қатар Dragonblood шабуылдары сияқты жаңама арналар арқылы шабуылдарға осалдығын көрсетеді. Өз кезегінде, LTE халықаралық мобильді абоненттік идентификаторды (IMSI Catching) ұстап алу қаупіне және желі дәрежесін 3G/2G-ге дейін төмендету шабуылдарына ұшырайды, бұл шабуылдаушыларға қызмет көрсетуден бас тартуға және трафикті ұстап алуға мүмкіндік береді.

Нәтижелер ескірген стандарттардан бас тарту, WPA3 аутентификация механизмдерін жақсарту және LTE сигналдық хаттамаларын жақсарту қажеттілігін көрсетеді. Бұл жұмыс сымсыз байланыс қауіпсіздігін арттыруға және қауіпсіз мобильді құрылғыларды жобалауға ықпал етеді.

Түйін сөздер: *Wi-Fi, LTE, желілік қауіпсіздік, қауіпсіздікті талдау, WEP, WPA, WPA2, WPA3, енуді тестілеу, бағдарламалық жасақтамамен анықталған радио.*

Кіріспе

Смартфондарды қорғаудың жеткіліксіз деңгейі оларды құпия деректердің ағып кетуіне, рұқсатсыз бақылауға және маңызды жүйелердің бұзылуына ықпал ететін кибершабуылдарға осал етеді. Сымсыз желілердегі осалдықтар трафикті ұстап алуға және шабуылдаушылардың рұқсатсыз кіруіне жағдай жасай отырып, осы тәуекелдерді едәуір арттырады. Қауіпсіз мобильді құрылғыларды әзірлеу Wi-Fi және LTE/5G қоса алғанда, сымсыз байланыс технологияларының осалдықтарын егжей-тегжейлі талдауды қажет етеді. Бұл стандарттар тұрақты байланыс ұсынғанымен, олардың қауіпсіздігі телекоммуникациялық жүйелердің қарқынды дамуы жағдайында күрделі мәселелердің бірі болып қала береді. Өткізу қабілеті мен сенімділігіне қойылатын талаптардың өсуі, ұялы байланыс буындарының өзгеруі (3G-ден 5G-ге дейін), сондай-ақ мобильді құрылғылардың технологиялық базасының эволюциясы оларды қорғауды қамтамасыз ету міндетін қиындатады.

Check Point мәліметтері бойынша [1], ұйымдардың 29%-ы Wi-Fi желілері арқылы шабуылдарға тап болды, мобильді желілер (LTE/5G) байланыс инфрақұрылымына жасалған барлық шабуылдардың 15% құрады, оқиғалар санының өсуі өткен жылмен салыстырғанда 18% құрады. Зиянкелтірушілердің біліктілігінің артуы жағдайды нашарлатады: WEP және WPA хаттамалары оңай бұзылады [2], WPA2 аутентификацияға осал [3], ал WPA3 іске асыруда әлсіз жақтары бар [4]. GSM/LTE-де 4G және 5G желілері IMSI-ді ұстап қалуға және 2G [5], [6] қайта бағыттауға ұшырайды, бұл құпиялылыққа қауіп төндіреді. Осы осалдықтарды есепке алу пайдалану тәуекелдерін азайта отырып, қауіпсіз смартфон жасауға мүмкіндік береді.

Зерттеу мақсаты – Wi-Fi (WEP, WPA, WPA2, WPA3) және LTE сымсыз желілерінің осалдықтарына теориялық және практикалық талдау жүргізу, оларды тестілеу әдістемесін әзірлеу, түпнұсқа сценарийлерін жасау арқылы пентестинг құралдарының функционалдығын

кеңейту, сондай-ақ қорғалған смартфонды жобалау контекстінде осы технологиялардың қорғалу деңгейін бағалау.

Зерттеу аясында келесі гипотезалар тұжырымдалды және тексерілді:

1. қолданыстағы Wi-Fi және LTE хаттамалары технологиялардың дамуы мен зиянкелтірушілердің біліктілігінің өсуіне байланысты заманауи кибершабуылдардан қорғаудың жеткіліксіз деңгейін қамтамасыз етеді;
2. практикалық енуді тестілеу сымсыз желілердің қауіпсіздік деңгейін нақты қауіп-қатерлерді модельдеу арқылы дәлірек бағалауға мүмкіндік береді, соның ішінде деректерді ұрлау, Құпия сөздерді ашу және қосылымды аз қорғалған қауіпсіздік деңгейлеріне (redirect attacks) мәжбүрлеп қайта бағыттауға негізделген шабуылдар.

Зерттеудің ғылыми үлесі осалдықтарды талдау және Wi-Fi (WEP, WPA, WPA2, WPA3) және LTE желілерінің қауіпсіздігін тексеру бойынша жаңа эксперименттік деректерді алу болып табылады. Зерттеу желілік конфигурациялардың қауіпсіздік деңгейін арттыру үшін олардың қолданылуын көрсететін арнайы әзірленген стендтер мен әдістерді қолдану арқылы жүргізілді. Желілік құрылғыларды орнату және қорғалған мобильді құрылғыларды жобалау бойынша әзірленген ұсыныстар телекоммуникациялық технологиялардың қарқынды дамуы жағдайында пайдаланушылардың қауіпсіздігін арттыруға ықпал етеді.

Протоколдардың осалдығын теориялық талдау эксперименттік стендтер мен сынақ әдістерін әзірлеумен толықтырылды, олардың нәтижелері WEP және WPA2 протоколдары инициализация және аутентификация векторларын ұстап қалу арқылы шабуылдарға осал екенін көрсетті, ал LTE IMSI ұстап қалуға және қосылымды аз қорғалған желілерге мәжбүрлеп қайта бағыттауға бейім.

Байланысқан жұмыстар

Wi-Fi және LTE сымсыз желілерінің осалдығын зерттеу (теориялық және практикалық) аспектілерді қамтиды. Schmitt және Raghavan [7] сигнал деңгейіндегі шабуылдар (signaling layer attacks) арқылы халықаралық мобильді абоненттік идентификаторды (International Mobile Subscriber Identity, IMSI) ұстап алу мүмкіндігін анықтау арқылы LTE желілерінде құпиялылықты жақсарту тәсілін ұсынды. Shaik және т.б. [5] жалған базалық станцияларды қолдана отырып, 4G/LTE желілерінде деректерді ұстап алу және қызмет көрсетуден бас тарту (Denial of Service, Qos) шабуылдарын көрсетті. Raza және т. б. [6] басқару деңгейінде (control plane) шифрлау кілттерін қайта орнату шабуылдарынан LTE қауіптерін анықтады.

Зерттеу жұмысында [8] 4G және 5G желісінің шабуылдарының үш түрі сипатталған:

- ToRPEDO (Tracking via Paging Message Distribution немесе пейджингтік хабарламаларды тарату арқылы бақылау) пейджингтік хаттамаларды талдау арқылы орынды анықтайды;
- PIERCER (Persistent Information Exposure by the Core Network немесе желінің ядросы арқылы ақпаратты үнемі ашып отыру) IMSI мен телефон нөмірі арасында байланыс орнатады;
- IMSI-Cracking шифрланған IMSI-ді ашу үшін толық іріктеу (brute-force) әдісін қолданады.

Nohl [2] GSM желілеріндегі A5/1 алгоритміне криптоталдау жүргізіп, шифрлау кілттерін алу үшін алдын ала есептелген кестелерді қолданатын шабуылды әзірледі.

Wi-Fi желілері үшін жұмыс авторлары [3] WPA2 және WPA 3-те аутентификация шабуылының мүмкіндігін көрсетті. Halbouni және т.б. WPA3 протоколының артықшылықтары мен кемшіліктерін парольге негізделген аутентификация механизмінің осалдығын және парольді аутентификациямен кілттерді сәйкестендіруді (Simultaneous authentication of Equals, SAE) көрсете отырып қорытындылады [4]. Baray және Ojha [9] WEP, WPA, WPA2 және WPA3 осалдықтарын зерттеп, Aircrack-ng утилитасы арқылы WEP және WPA2-ге зиян келтірудің жеңілдігін растады және ескірген құрылғылармен үйлесімділікте WPA3 қорғанысын WPA2-ге дейін төмендету қаупін анықтады.

1-кесте зерттеулерде сипатталған шабуылдар құралдары мен түрлерін қорытындылайды.

Біздің зерттеуіміз осы жұмыстарға сүйенеді, бірақ кешенді тәсілмен ерекшеленеді: Wi-Fi және LTE желілерінің осалдықтарын талдау, енуді тестілеуге арналған стендтер мен сценарийлерді әзірлеу (penetration testing), қауіпсіз смартфондарды жобалау кезінде ескеру қажет осалдықтарды анықтауға бағытталған. Әдістерге трафикті ұстау, базалық станцияларды эмуляциялау және SDR (USRP, HackRF) және утилиталар (Aircrack-ng, Wireshark, YateBTS) арқылы протоколдарды талдау кіреді. Осы зерттеудегі SDR таңдауы олардың әмбебаптығына негізделген, бұл Wi-Fi және LTE желілерінің радио интерфейсіне шабуылдарды модельдеуге мүмкіндік береді, бұл келесі тәсілдерге сәйкес келеді [5] және [6].

Кесте 1 – Сымсыз шабуылдарға шолу

Дереккөз	Желілік хаттама	Шабуыл түрі	Құралдар	Шабуылдың мақсаты
[2]	GSM	A5/1 кілттерін ұстап алу	Радио жабдықтар, алдын-ала есептелген кестелер	Деректердің ағып кетуі
[5]	4G/LTE	DoS (Denial of Service), деректерді ұстап алу	Жалған базалық станциялар, SDR USRP	Қызмет көрсетуден бас тарту, деректердің ағып кетуі
[6]	4G LTE	Шифрлау кілттерін қайта орнату	SDR HACKRF One	LTE компрометациясы
[8]	4G/5G	ToRPEDO (Tracking via Paging Message Distribution)	Сниффер, жалған базалық станция	Орналасқан жерді бақылау
[8]	4G/5G	PIERCER (Persistent Information Exposure by the Core Network)	Сниффер, жалған базалық станция	IMSI телефон нөмірімен байланысы
[8]	4G/5G	IMSI-Cracking	Сниффер	Раскрытие IMSI
[3]	Wi-Fi (WPA2/WPA3)	Аутентификациядан шығару	Көрсетілмеген	Отключение клиентов
[4]	Wi-Fi (WPA3)	SAE-ге шабуылдар (Simultaneous Authentication of Equals)	Әдебиеттерге талдау	WPA3 компрометациясы
[9]	Wi-Fi (WEP/WPA2)	Аутентификация пакеттерін ұстау, WPA3 қорғанысын төмендету	Aircrack-ng	Желіге қол жеткізу

Зерттеу әдістемесі

Сымсыз желілердің осалдығын талдау үшін екі эксперимент жоспарланды және жүзеге асырылды: Wi-Fi протоколдарын тестілеу және LTE желілерін зерттеу және смартфонды жобалауда қолданылатын сымсыз желілердің жалпы тұжырымдамасы мен қауіпсіздік талаптары қарастырылды. Эксперименттерді "WebTotem" ЖШС R&D бөлімі төменде сипатталған стендтер мен бағдарламалық қамтамасыз етуді пайдалана отырып жүргізді.

Смартфонды жобалауда қолданылатын сымсыз желілердің жалпы тұжырымдамасы мен қауіпсіздік талаптары

Wi-Fi (Wireless Fidelity) – сымдарды пайдаланбай Интернетке қол жеткізуді және деректермен алмасуды қамтамасыз ететін сымсыз деректерді беру технологиясы. Ол 2,4 ГГц және 5 ГГц жиіліктерінде жұмыс істейді, құрылғыларды (смартфондар, ноутбуктер, планшеттер) кіру нүктелеріне (маршрутизаторларға) қосады.

Wi-Fi желілеріндегі деректерді қорғау үшін WEP, WPA, WPA2 және WPA 3 шифрлау протоколдары қолданылады. 1997 жылы қабылданған WEP RC4 алгоритмін және 24 биттік инициализация векторын қолданады, бірақ тосқауыл шабуылдарына осал. WPA (2003) TKIP енгізді, бірақ сонымен бірге толық қорғалмаған. WPA2 (2004) CCMP көмегімен AES-128 қолданады, бұл қауіпсіздікті айтарлықтай жақсартады. WPA3 (2018) SAE, кәсіпорын желілері үшін 192 биттік шифрлауды және сөздік шабуылынан қорғауды жақсартты.

LTE (Long-Term Evolution) – жүктеу жылдамдығын 300 Мбит/с дейін қамтамасыз ететін 4G стандарты, Қазақстанда 800 МГц (кең қамту), 900 МГц (жақсартылған ену қабілеті), 1800 МГц (жылдамдық пен қамтудың оңтайлы үйлесімі), 2100 МГц (өткізу қабілеттілігінің жоғарылауы) және 2600 МГц (ең жоғары өткізу қабілеттілігі) диапазондары пайдаланылады деректерді беру жылдамдығы).

LTE қауіпсіздік жүйесі мыналарды қамтиды:

– SIM картасы арқылы аутентификация (рұқсатсыз кіруден қорғау).

– Деректерді шифрлау (AES, SNOW 3G).

– Сигналдық трафикті қорғау (хабарламалардың өзгеруіне жол бермеу).

– Уақытша идентификаторларды (IMSI) пайдалану (бақылаудан қорғау).

– IPsec қолдану (қорғалған деректерді беру).

Жоғары қорғаныс деңгейіне қарамастан, LTE IMSI-Catcher (идентификаторды ұстау), сигнал шабуылдары (DoS), сигналды өшіру (jamming) және шифрлау жеткіліксіз болған кезде трафикті талдау сияқты шабуылдарға бейім.

Смартфонды жобалауда қолданылатын сымсыз желілердің енуіне практикалық тестілеу және осалдықтарды анықтау

Смартфонды жобалауда қолданылатын сымсыз желілер туралы ақпаратты талдау негізінде зерттеу тобы практикалық тестілеудің келесі негізгі кезеңдерін өткізуге шешім қабылдады:

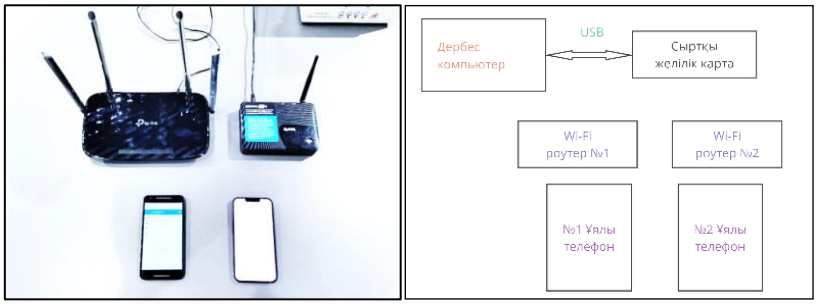
– Wi-Fi сымсыз желісінің осалдығына зерттеу жүргізу;

– LTE сымсыз байланыс осалдығына зерттеу жүргізу.

Эксперименттің мақсаты WEP, WPA, WPA2 және WPA3 протоколдарының деректерді ұстап алу шабуылдарына төзімділігін тексеру болды. Тестілеу үшін сынақ стенді (2-кесте, 1-сурет) қолданылды, оның құрамына дербес компьютер, екі Wi-Fi маршрутизаторы, сыртқы желілік карта және әртүрлі операциялық жүйелері бар мобильді құрылғылар кірді. Aircrack-ng және Wireshark бағдарламалық жасақтамалары трафикті талдау және аутентификация пакеттерін ұстап алу (handshake capture) үшін пайдаланылды.

Кесте 2 – Wi-Fi тестілеуге арналған жабдық

№	Жабдық	Үлгі	Негізгі сипаттамалары
1	Дербес компьютер	Lenovo ThinkPad T-480s	Intel Core i7, 16 ГБ ОЗУ, Fedora 40
2	Сыртқы желі картасы	TP-Link TL-WN722N	Wi-Fi тестілеуге арналған жабдық
3	Wi-Fi-роутер №1	TP-Link Archer C6 AC1200	2,4/5 ГГц, WPA/WPA2, 867 Мбит/с (5 ГГц)
4	Wi-Fi-роутер №2	ZYXEL Keenetic 4G II	2,4 ГГц, WEP/WPA/WPA2, 150 Мбит/с
5	№ 1 Ұялы телефон	LG Nexus 5X	Wi-Fi 802.11 a/b/g/n/ac, Snapdragon 808
6	№ 2 Ұялы телефон	Apple iPhone 13	Wi-Fi 6, A15 Bionic, LTE MIMO 4×4



Сурет 1 – Зерттеуге пайдаланылған құрылғылардың фотосуреттері және Wi-Fi сымсыз желісінің осалдықтарын зерттеуге арналған сынақ стендінің құрылымдық сызбасы.

Әдістеме роутерлерді әртүрлі шифрлау протоколдарымен баптауды, мобильді құрылғыларды қосуды және кейіннен трафикті ұстап алуды қамтыды. WEP үшін инициализация векторлары (Initialization Vector, IV) талданды, WPA/WPA2 протоколдарының қауіпсіздігін талдау үшін аутентификация пакеттері зерттелді. WPA3 протоколы жағдайында деаутентификация шабуылдарына және байланыстың қауіпсіздік деңгейін төмендетуге бағытталған қайта бағыттау шабуылдарына (redirect attack) төзімділігі бағаланды.

Эксперимент 2 «LTE желісін зерттеу»

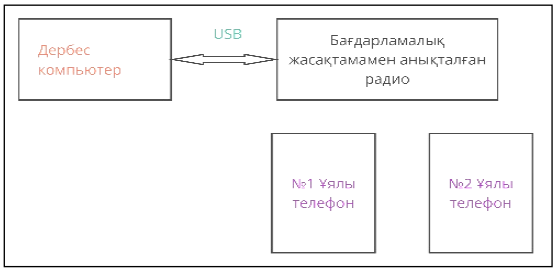
Мақсат LTE осалдықтарын, соның ішінде IMSI (International Mobile Subscriber Identity) және қызмет көрсетуден бас тарту (Denial of Service, DoS) шабуылдарын зерттеу болды. Бағдарламалық жасақтамамен анықталған радио (SDR, Software-Defined Radio) BladeRF 2.0, Ubuntu ОЖ дербес компьютері және мобильді құрылғылары (Nokia TA-1034, Xiaomi POCO3) бар стенд қолданылды (кесте. 3, сурет. 2). Виртуалды базалық станцияны іске асыру үшін YateBTS (Yet Another Telephony Engine base Transceiver Station) бағдарламалық жасақтамасы қолданылды.

Әдістеме GSM/LTE желісін имитациялау үшін YateBTS баптауды, құрылғыларды қосуды және сигналдық трафикті талдау арқылы IMSI ұстап алуды қамтыды. Қосымша түрде мобильді телефонды төменгі деңгейдегі желіге (мысалы, 4G-ден 3G-ге) ауыстыру арқылы байланыстың қауіпсіздік деңгейін төмендету шабуылдары (redirect attack) тексерілді [10-12].

Екі экспериментті де қайталап жасауға болады: жабдық пен бағдарламалық жасақтама жалпыға қол жетімді және қадамдар егжей-тегжейлі құжатталған, бұл ұқсас жағдайларда тестілеуді қайталауға мүмкіндік береді.

Кесте 3 – LTE тестілеуге арналған жабдық

№	Жабдық	Үлгі	Негізгі сипаттамалары
1	Дербес компьютер	Lenovo ThinkPad T-480s	Intel Core i7, 16 ГБ ОЗУ, Ubuntu
2	SDR құрылғысы	Nuand BladeRF 2.0	47 МГц–6 ГГц, 2×2 MIMO, 61,44 МГц дискретизациясы
3	№ 1 Ұялы телефон	Nokia TA-1034	GSM, MediaTek MT6261D, 4 МБ ОЗУ
4	№ 2 Ұялы телефон	Xiaomi POCO3	4G/5G, Snapdragon 870, 4520 мА·ч



Сурет 2 – LTE сымсыз желісінің осалдығын зерттеуге арналған стендтің құрылымдық схемасы

Нәтижелер

Сымсыз желі протоколдарының теориялық талдауы

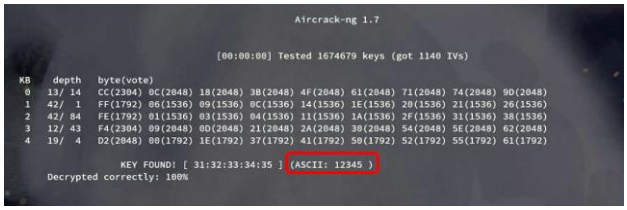
Бірінші кезеңде негізгі қауіптерді анықтау және енуді тестілеу эксперименттерін жоспарлау үшін зерттелетін сымсыз байланыс хаттамаларына теориялық талдау жүргізілді. 4-кесте теориялық талдау нәтижелерін қорытындылайды.

Кесте 4 – Хаттамаларға және олардың негізгі қауіптеріне шолу

Хаттама	Шифрлау әдісі (Encryption Method)	Негізгі қауіп (Key Threat)
WEP	RC4	Инициализация векторларын ұстап алу (IV interception)
WPA	TKIP (Temporal Key Integrity Protocol)	TKIP-тің шектеулі төзімділігі (Limited TKIP resilience)
WPA2	AES (Advanced Encryption Standard)	Аутентификация пакеттерін ұстап алу (Handshake capture)
WPA3	AES	Жанама арналар (Side-channel attacks)
LTE	AES, SNOW 3G	IMSI ұстау, қорғаныс деңгейін төмендету (IMSI interception, downgrade)

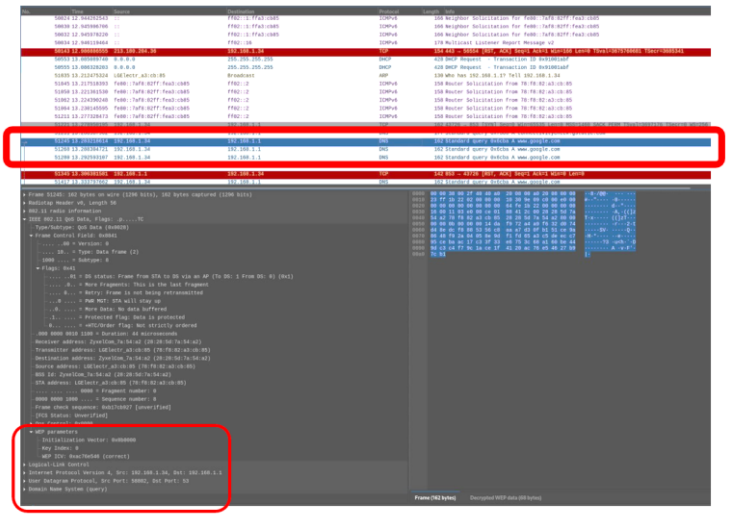
Wi-Fi желісінің протоколдарының қауіпсіздігін тексеру нәтижелері

Желінің Wi-Fi протоколдарын тестілеу деректерді ұрлау шабуылдарына (data interception) әр түрлі төзімділікті көрсетті. "12345" (64 бит) паролі бар WEP протоколы үшін Aircrack-ng көмегімен 500 мың инициализация векторы ұсталды, бұл шифрлау кілтін 4 секундта ашуға мүмкіндік берді (7-суретті қараңыз). Wireshark-тағы трафикті талдау интернет-ресурстарға қол жетімділікті анықтады (мысалы, www.google.com) транскрипциядан кейін (3-сурет).



Сурет 3 – WEP протоколының құпия сөзін шифрдан шығару

WPA2 үшін «17384957» паролімен аутентификация пакеттерін (handshake capture) ұстап алу бірнеше секундты алды, өйткені деаутентификация шабуылы (deauthentication attack) Aireplay-ng көмегімен орындалды, басқару кадрларын қорғауға (Management Frame Protection, MFP) қарамастан. Кілт алдын ала жасалған сандық сөздік (dictionary) және құрылған скрипт көмегімен ашылды (4, 5-сурет). WPA және WPA3 үлкен тұрақтылық көрсетті, алайда WPA3 үшін аутентификация процесінде (Simultaneous Authentication of Equals, SAE) деректердің ағуына (data leaks) байланысты жанама арналар арқылы (side-channel attacks) шабуыл жасауға осалдық анықталды.



Сурет 4 – Ұстап алынған пакеттерден шифрланған деректерді талдау

```
with open("wordlist-num.txt", "w+") as f:
    for i in range(100_000_000):
        f.write("{:08d}\n".format(i))
```

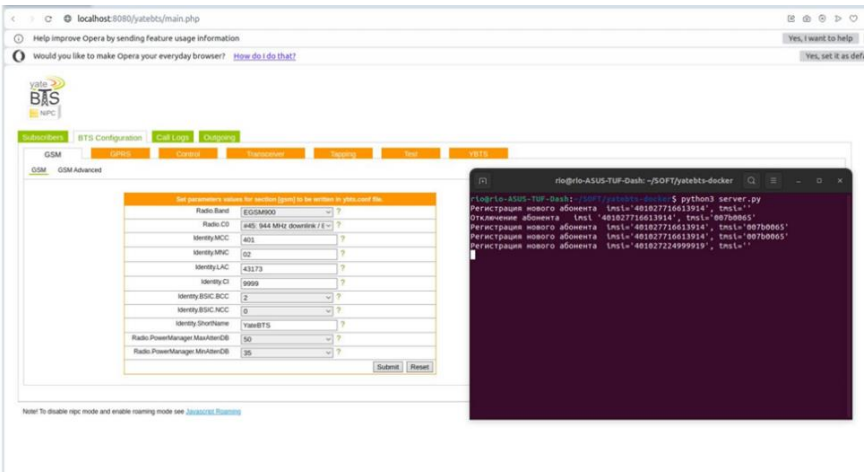
Сурет 5 – Python бағдарламалау тілінде сөздік құруды жүзеге асыру

LTE желісінің тестілеу нәтижелері

YateBTS (Yet Another Telephony Engine base Transceiver Station) бағдарламалық жасақтамасын және BladeRF 2.0 бағдарламалық жасақтамасымен анықталған радио құралын қолдана отырып, LTE желісінде виртуалды базалық станция сәтті орналастырылды. Nokia TA-1034 және Xiaomi POCO3 құрылғылары IMSI арқылы анықталған 6613914 және 4999919 нөмірлерімен қосылды (6-сурет). IMSI (IMSI interception) ұстап алу сигналдық трафикті талдау (signaling traffic) арқылы жүзеге асырылады және құрылғылар арасындағы қоңырау расталады. Тестілеу қауіпсіздігі төмен желілердегі ұялы байланыс пакеттерін қайта бағыттаумен байланыс деңгейінің төмендеуі (redirect attack) шабуылдарының осалдығын анықтады. LTE желісінің осалдығын талдау нәтижелерінің сандық параметрлері 5-кестеде келтірілген.

Кесте 5 – LTE тестілеу нәтижелері

Құрылғы (Device)	IMSI ұстап алу (IMSI Interception)	Желідегі қоңырау (Call in Network)	Осалдық (Vulnerability)
Nokia TA-1034	Иә (Yes)	Иә (Yes)	3G дейін төмендету
Xiaomi POCO3	Иә (Yes)	Иә (Yes)	3G дейін төмендету



Сурет 6 – Ұялы телефондарды виртуалды базалық станцияға қосу

Нәтижелерді талқылау

Нәтижелер WEP протоколының инициализация векторларын (IV interception) ұстауға жоғары осалдығын растайды, бұл оны заманауи желілер үшін жарамсыз етеді. WPA2 екінші нұсқасының ХАТТАМАСЫ жетілдірілген AES шифрлау стандартын (Advanced Encryption Standard) пайдаланғанына қарамастан, үйлесімділік пен басқару кадрларын қорғауды (Management Frame Protection, MFP) жүзеге асырудағы кемшіліктерге байланысты аутентификация пакеттерін (handshake capture) ұстауға бейім болып қалады. Үшінші нұсқадағы Wi-Fi желісіне қорғалған қол жетімділік протоколы (WPA3) бір мезгілде тең аутентификация механизмінің (Simultaneous authentication of Equals, SAE) арқасында тұрақтылықтың жоғарылауын көрсетеді, бірақ жанама арналар арқылы шабуылдардан (side-channel attacks) қауіптер қосымша талдауды қажет етеді, бұл Halbouni және басқалардың тұжырымдарына сәйкес келеді. [4].

LTE (Long-Term Evolution, ұзақ мерзімді эволюция) желілерінде IMSI (IMSI interception) ұстап алу және GSM (Global System for Mobile Communications, global system for mobile communications) дейін төмендету мүмкіндігі сигналдық хаттамалардың (signaling protocols) әлсіздігін көрсетеді, бұл Shaik және т.б. нәтижелерін растайды. [5]. Бұл құпиялылыққа (privacy) және деректердің тұтастығына (data integrity) қауіп төндіреді, әсіресе аралас желілердегі смартфондар үшін.

Нәтижелер смартфондардың қауіпсіздігіне кешенді көзқарастың қажеттілігін көрсетеді, соның ішінде ескірген протоколдардан бас тарту, WPA3 жетілдіру және LTE-ді ұялы байланысты қорғауды төмендету деңгейлеріне қайта бағыттау шабуылдарынан қорғау.

6-кесте сымсыз байланыс желілерінің осалдықтарын талдау нәтижелерін жинақтайды.

Кесте 6 – Осалдықтарды салыстыру және ұсыныстар әзірлеу

Хатамма	Негізгі қауіптер	Шабуыл жылдамдығы	Ұсыныс
WEP	Инициализация векторларын ұстап алу (IV interception)	Өте жоғары (Very high)	Пайдаланудан бас тарту (Phase-out)
WPA2	Аутентификация пакеттерін ұстап алу (Handshake capture)	Жоғары (High)	WPA3-ке көшу (Transition to WPA3)
WPA3	Жанама арналар (Side-channel attacks)	Төмен (Low)	SAE жақсарту (Enhance SAE implementation)
LTE	IMSI ұстап а, қайта бағыттау (IMSI interception, redirect)	Орташа (Moderate)	Сигналдық хаттамаларды күшейту (Strengthen signaling protocols)

Қорытынды

Зерттеу заманауи мобильді құрылғыларда қолданылатын сымсыз байланыс хаттамаларында айтарлықтай осалдықтарды анықтады. Эксперименттік нәтижелер инициализация векторларының бұзылуының жоғары ықтималдығына байланысты WEP протоколының толық тиімсіздігін растады. Жетілдірілген AES шифрлау алгоритмін қолданғанына қарамастан, WPA2 протоколы аутентификация пакеттеріне (handshake packets) шабуылдарға осал болып қала береді. WPA 3 протоколы қауіпсіздікті жақсартудың айтарлықтай әлеуетіне ие, бірақ жанама арналарды талдауға негізделген шабуылдардан қорғау үшін аутентификация механизмдерін жетілдіруді қажет етеді.

LTE желілерінде пайдаланушылардың құпиялылығының бұзылу қаупі анықталды, бұл халықаралық мобильді абонент идентификаторын (IMSI) ұстап алу және құрылғыны ескірген, қауіпсіздігі төмен байланыс стандарттарына мәжбүрлі түрде ауыстыру мүмкіндігімен байланысты. Бұл осалдықтарды жою үшін сигналдық протоколдарды жетілдіру қажеттігін көрсетеді.

Енуді тексеруге арналған эксперименттік стендтер мен сценарийлер мобильді құрылғылардың қауіпсіздігіне нақты қауіп төндіретін нәтижелердің қайталануын қамтамасыз етті. Зерттеу неғұрлым қорғалған стандарттарға көшудің өзектілігін көрсетеді және практикалық шараларды ұсынады: ескірген хаттамаларды пайдаланудан шығару, WPA3 модернизациясы және LTE желілеріндегі қорғаныс механизмдерін күшейту. Осы ұсыныстарды іске асыру күрделі кибершабуылдар жағдайында мобильді құрылғылардың қауіпсіздік деңгейін арттыруға мүмкіндік береді.

Әдебиеттер тізімі
1. Check Point Software, Cyber Security Report 2023, Check Point Cyber Hub, 2023. [Online]. Доступно: https://www.checkpoint.com/cyber-hub/cyber-security-report/. [Қол жеткізілген күні: 2025 жылғы 24 қаңтар].
2. Nohl K. Attacking phone privacy in Black Hat USA / K. Nohl – 2010. – P. 1-6.
3. Lounis K. Cut it: Deauthentication attacks on protected management frames in WPA2 and WPA3, in Foundations and Practice of Security (FPS 2021) / K. Lounis, S.H.H. Ding, M. Zulkernine // Cham: Springer. – 2022. – P. 241-256.
4. Halbouni A. Wireless security protocols WPA3: A systematic literature review / A. Halbouni, L.-Y. Ong, M.-C. Leow // IEEE Access. – 2023. – vol. 11. – P. 112438-112450.
5. Practical attacks against privacy and availability in 4G/LTE mobile communication systems / A. Shaik et al // in Proc. 23rd Annu. Netw. Distrib. Syst. Security Symp. (NDSS). – 2016. – P. 1-16.
6. On key reinstallation attacks over 4G LTE control-plane: Feasibility and negative impact / M.T. Raza et al // Anwar in Proc. 37th Annu. Comput. Security Appl. Conf. – 2021. – P. 877-886.
7. Schmitt P. Pretty good phone privacy / P. Schmitt, B. Raghavan // in Proc. 30th USENIX Security Symp. – 2021. – P. 1737-1754.
8. Privacy attacks to the 4G and 5G cellular paging protocols using side channel information / S.R. Hussain et al // in Proc. Netw. Distrib. Syst. Security Symp. (NDSS). – 2019. – P. 1-15.
9. Baray E. WLAN security protocols and WPA3 security approach measurement through aircrack-ng technique / E. Baray, N.K. Ojha // in Proc. 5th Int. Conf. Comput. Methodologies Commun. (ICCMC). – 2021. – P. 23-30.
10. Vanhoef M. Dragonblood: Analyzing the Dragonfly Handshake of WPA3 and EAP-pwd / M. Vanhoef, E. Ronen // 2020 IEEE Symposium on Security and Privacy (SP). – IEEE, 2020. – P. 517-533.
11. Vanhoef M. Key reinstallation attacks: Forcing nonce reuse in WPA2 / M. Vanhoef, F. Piessens // Proceedings of the 2017 ACM SIGSAC conference on computer and communications security. – 2017. – P. 1313-1328.
12. Lin H. LTE Redirection Attack-Forcing Targeted LTE Cellphone into Unsafe Network / H. Lin // Unicorn Team-Radio and Hardware Security Research. – 2016.

Алғыс

Бұл зерттеу Қазақстан Республикасының Ғылым және жоғары білім министрлігі Ғылым комитеті тарапынан қаржыландырылды (№ BR249014/0224 гранты).

А.К. Шайханова[1,2]*, Р.А. Буденов[2], О.Ш. Сатиев[2], Д.А. Тлепов[2], А.К. Токкулиева[1]
[1]Евразийский национальный университет им. Л.Н. Гумилева,
Республика Казахстан, Астана, ул. К.Сатпаева, 2
[2]ТОО «WebTotem»,
Республика Казахстан, Астана, проспект Кабанбай Батыра 51/1
*e-mail: aigul.shaikhanova@gmail.com

АНАЛИЗ УЯЗВИМОСТЕЙ БЕСПРОВОДНЫХ СЕТЕЙ WI-FI И LTE ДЛЯ ПРОЕКТИРОВАНИЯ ЗАЩИЩЁННОГО СМАРТФОНА

В данной работе представлены результаты практического анализа уязвимостей беспроводных сетей Wi-Fi (WEP, WPA, WPA2, WPA3) и LTE в контексте проектирования защищённого смартфона. Исследование проведено с использованием комплекса инструментов, включая Aircrack-ng, Wireshark, YateBTS и программно-определяемого радио BladeRF 2.0, что позволило детально изучить механизмы атак и устойчивость современных протоколов к различным типам угроз.

Экспериментальная часть включала разработку стендов и автоматизированных скриптов для тестирования на проникновение. Анализ показал, что протокол WEP обладает критическими уязвимостями и может быть взломан всего за 4 секунды. WPA2 оказался подвержен атакам, связанным с перехватом пакетов аутентификации, что делает возможным реализацию атак типа «человек посередине» (MITM). Несмотря на усовершенствования, WPA3 также демонстрирует уязвимость к атакам через побочные каналы, например, атакам Dragonblood. В свою очередь, LTE подвергается рискам перехвата международного идентификатора мобильного абонента (IMSI Catching) и атакам понижения ранга сети до 3G/2G, что позволяет злоумышленникам проводить атаки на отказ в обслуживании и перехватывать трафик.

Полученные результаты подчёркивают необходимость отказа от устаревших стандартов, улучшения механизмов аутентификации WPA3 и усовершенствования сигнальных протоколов LTE. Настоящая работа вносит вклад в повышение безопасности беспроводных коммуникаций и проектирование защищённых мобильных устройств.

Ключевые слова: *Wi-Fi, LTE, сетевая безопасность, анализ безопасности, WEP, WPA, WPA2, WPA3, тестирование на проникновение, программно-определяемое радио.*

A.K. Shaikhanova[1,2]*, R.A. Budenov[2], O.Sh. Satiev[2], D.A. Tlepov[2], A.K. Tokkuliyeva[1]
[1]L.N. Gumilyov Eurasian National University,
Republic of Kazakhstan, Astana, K.Satpayev str., 2
[2]WebTotem LLP,
Republic of Kazakhstan, Astana, 51/1 Kabanbai Batyr Avenue
*e-mail: aigul.shaikhanova@gmail.com

VULNERABILITY ANALYSIS OF WI-FI AND LTE NETWORKS FOR SECURE SMARTPHONE DESIGN

This paper presents the results of practical vulnerability analysis of Wi-Fi (WEP, WPA, WPA2, WPA3) and LTE wireless networks in the context of designing a secure smartphone. The study was conducted using a set of tools, including Aircrack-ng, Wireshark, YateBTS and software-defined radio BladeRF 2.0, which allowed to study in detail the attack mechanisms and resistance of modern protocols to various types of threats.

The experimental part included the development of stands and automated scripts for penetration testing. The analysis showed that the WEP protocol has critical vulnerabilities and can be compromised in just 4 seconds. WPA2 was susceptible to attacks related to authentication packet interception, making man-in-the-middle (MITM) attacks possible. Despite the improvements, WPA3 also shows vulnerability to side-channel attacks such as Dragonblood attacks. LTE, on the other hand, is vulnerable to International Mobile Subscriber Identity (IMSI Catching) and 3G/2G downgrade attacks, allowing attackers to conduct denial of service attacks and intercept traffic.

The results underscore the need to abandon outdated standards, improve WPA3 authentication mechanisms and enhance LTE signalling protocols. This paper contributes to improving the security of wireless communications and the design of secure mobile devices.

Key words: *Wi-Fi, LTE, Network Security, security analysis, WEP, WPA, WPA2, WPA3, Penetration Testing, software defined radio (SDR).*

Сведения об авторах

Айгуль Кайрулаевна Шайханова – PhD, профессор кафедры информационной безопасности; Евразийский национальный университет имени Л.Н. Гумилева; координатор научных проектов ТОО «WebTotem», г. Астана, Казахстан; e-mail: aigul.shaikhanova@gmail.com. ORCID: https://orcid.org/0000-0001-6006-4813.

Руслан Аримбаевич Буденов – магистр технических наук, Инженер-электронщик ТОО «WebTotem», г. Астана, Казахстан; e-mail: akarkin@mail.ru. ORCID: https://orcid.org/0009-0003-9088-3221.

Олжас Шагзадович Сатиев – старший эксперт по информационной безопасности ТОО «WebTotem», г. Астана, Казахстан; e-mail: os@wtotem.com. ORCID: https://orcid.org/0009-0005-2684-1718.

Данир Амангельдинович Тлепов – магистр технических наук, Научный сотрудник ТОО «WebTotem», г. Астана, Казахстан; e-mail: tdanir@cert.kz. ORCID: https://orcid.org/0009-0003-3774-8389.

Айжан Конурбаевна Токкулиева – магистр технических наук, докторант 1 курса специальности «Системы информационной безопасности», Евразийский национальный университет имени Л.Н. Гумилева; младший научный сотрудник ТОО «WebTotem», г. Астана, Казахстан; e-mail: aizhantokkuliyeva1983@gmail.com. ORCID: https://orcid.org/0000-0002-5019-2413.

Авторлар туралы мәліметтер

Айгуль Кайрулаевна Шайханова – PhD, ақпараттық қауіпсіздік кафедрасының профессоры; Л.Н. Гумилёв атындағы Еуразия ұлттық университеті; «WebTotem» ЖШС ғылыми жобалардың үйлестірушісі, Астана қ., Қазақстан; e-mail: aigul.shaikhanova@gmail.com. ORCID: https://orcid.org/0000-0001-6006-4813.

Руслан Аримбаевич Буденов – техника ғылымдарының магистрі, «WebTotem» ЖШС Инженер-электроник, Астана қ., Қазақстан; e-mail: akarkin@mail.ru. ORCID: https://orcid.org/0009-0003-9088-3221.

Олжас Шагзадович Сатиев – «WebTotem» ЖШС Ақпараттық қауіпсіздік жөніндегі аға сарапшысы, Астана қ., Қазақстан; e-mail: os@wtotem.com. ORCID: https://orcid.org/0009-0005-2684-1718.

Данир Амангельдинович Тлепов – техника ғылымдарының магистрі, «WebTotem» ЖШС ғылыми қызметкері, Астана қ., Қазақстан; e-mail: tdanir@cert.kz. ORCID: https://orcid.org/0009-0003-3774-8389.

Айжан Конурбаевна Токкулиева – техника ғылымдарының магистрі, «Ақпараттық қауіпсіздік жүйелері» мамандығының 1 курс докторанты, Л.Н. Гумилёв атындағы Еуразия ұлттық университеті; «WebTotem» ЖШС кіші ғылыми қызметкері, Астана қ., Қазақстан; e-mail: aizhantokkuliyeva1983@gmail.com. ORCID: https://orcid.org/0000-0002-5019-2413.

Information about the authors

Aigul Kairulaevna Shaikhanova* – PhD, Professor of the Department of Information Security; L.N. Gumilyov Eurasian National University; Coordinator of scientific projects of WebTotem LLP, Astana, Kazakhstan; e-mail: aigul.shaikhanova@gmail.com. ORCID: https://orcid.org/0000-0001-6006-4813.

Ruslan Arimbaevich Budenov – Master of Technical Sciences, Electronics Engineer, WebTotem LLP, Astana, Kazakhstan; e-mail: akarkin@mail.ru. ORCID: https://orcid.org/0009-0003-9088-3221 .

Olzhas Shagzadovich Satiev – Senior Information security Expert at WebTotem LLP, Astana, Kazakhstan; e-mail: os@wtotem.com. ORCID: https://orcid.org/0009-0005-2684-1718.

Danir Amangeldinovich Tlepov – Master of Technical Sciences, Researcher at WebTotem LLP, Astana, Kazakhstan; e-mail: tdanir@cert.kz. ORCID: https://orcid.org/0009-0003-3774-8389.

Aizhan Konurbaevna Tokkuliyeva – Master of Technical Sciences, 1st year doctoral student, specialty «Information Security Systems», L.N. Gumilyov Eurasian National University; Junior Researcher at WebTotem LLP, Astana, Kazakhstan; e-mail: aizhantokkuliyeva1983@gmail.com. ORCID: https://orcid.org/0000-0002-5019-2413.

Редакцияға енуі 03.03.2025
Өңдеуден кейін түсуі 05.03.2025
Жариялауға қабылданды 12.03.2025

https://doi.org/10.53360/2788-7995-2025-1(17)-5

IRTSTI: 28.23.15

A.K. Kalpen[1], E.T. Matson[2], A.K. Zhumadillayeva[1,3*], K.A. Dyussekeyev[3]
[1]Astana IT University,
Kazakhstan, Astana, Mangilik El 55/11, Block C1 QazExpo
[2]Purdue University,
West Lafayette, Indiana, USA
[3]L.N. Gumilyov Eurasian National University, Astana, Kazakhstan
*e-mail: Zhumadillayeva_ak@enu.kz

SEQUENCE RECOGNITION USING FINITE AUTOMATA WITH MACHINE LEARNING

Annotation: *Sequence recognition is a critical task across numerous disciplines. While traditional methods utilizing Finite State Machines (FSMs) offer a structured data representation and high interpretability, their flexibility is limited. Contemporary Machine Learning (ML) algorithms exhibit high accuracy but demand substantial computational resources. Combining these paradigms can enhance the effectiveness of complex sequence recognition. This study explores the integration of FSMs with ML techniques to address sequence analysis problems. Three distinct applications are examined: text classification (spam detection), recognition of genetic sequences related to Alzheimer's disease, and image-based gesture identification.*

For each, hybrid models were developed and tested, combining Deterministic Finite Automata (DFA), Non-deterministic Finite Automata (NFA), and ML algorithms such as Random Forest, Gradient Boosting, and Multilayer Perceptrons (MLP). Experimental results indicate that these hybrid models achieve performance comparable to traditional ML methods, and in some instances, yield more accurate predictions.

In spam classification, neural network models demonstrated the best results, with FSM-neural network combinations providing similar effectiveness.

For genetic sequence analysis, gradient boosting-based models exhibited the highest accuracy, with the inclusion of FSMs maintaining performance while enhancing interpretability.

In gesture recognition, neural network approaches proved most effective, but integrating FSMs with ensemble methods achieved a high level of predictive capability, surpassing conventional ML models.

In conclusion, the integration of FSMs and ML presents a promising avenue in sequence analysis. Future research could focus on optimizing model architectures and applying them to other domains requiring high-precision recognition of intricate structures.

Key words: *Finite State Machine, Machine Learning, Sequence Recognition, Hybrid Models, Genetic Sequence Analysis, Gesture Recognition, Text Classification.*