Scientific Journal of Astana IT University
ISSN (P): 2707-9031
ISSN (E): 2707-904X

DOI: 10.37943/AITU.2020.1.63687

F. Shinasilova
Master of Information Security systems
shinassilovaf@mail.ru, orcid.org/0000-0002-0635-872X
Eurasian National University after name L.N. Gumilyov, Kazakhstan

METHODS OF INFORMATION SECURITY IN WIRELESS NETWORKS

Abstract: The development of information technology sets the task of improving the reliability of computer networks. To study the security of networks, it is necessary to study the creation of network protocols, network architectures, and ways to strengthen security when transmitting information resources over a network. Network attacks, failures, and the failure of network devices are key factors affecting the security of information transmission in wireless networks.This article discusses methods for protecting information in wireless networks, including standards for authentication, encryption, and security. There are several security standards, but this article describes the effectiveness of those standards and the key principles used in those standards. It also outlines the principles of standards that ensure the confidentiality and integrity of data. That is, the TKIP protocol generates a new secret key for each packet of data transmitted, and one static WEP key is exchanged for about 500 billion possible keys. It can be used to encrypt this data set. The key generation mechanism has been modified. It consists of three components: a 128-bit Basic Key (TC), a packet number (TSC) and a MAC address of the carrier. The TKIP also uses a 48-bit initialization vector. It is used to prevent repeated use of vector IV. The TKIP algorithm uses a 48-bit (TSC) packet calculation. It keeps increasing. Well, the new 16-bit TSC IV is introduced (Figure 4). Thus, a mechanism is created that can block attacks.

Key words: wireless networking, security, authentication, asymmetric encryption, mesh portal, standard, Cisco Systems, WEP algorithm, TKIP protocol, MIC mechanism, IEEE 802.11i standard, authentication, EAP protocols.

Шинасилова Ф.
Информатика және ақпараттық қауіпсіздік, магистранты
shinassilovaf@mail.ru, orcid.org/0000-0002-0635-872X
Л.Н. Гумилев атындағы Еуразия ұлттық университеті, Қазақстан

СЫМСЫЗ ЖЕЛІЛЕРДЕ АҚПАРАТТАРДЫ ҚОРҒАУ ӘДІСТЕРІ

Аннотация: Ақпараттық технологиялардың дамуы компьютерлік желілердің сенімді түрде жұмыс істеуін жоғарылату тапсырмасын алға қояды. Желілердің қауіпсіздігін зерттеу үшін желі арқылы ақпараттық ресурстарды жіберу барысында желілік хаттамаларды, желілік архитектураларды, қауіпсіздікті нығайту тәсілдерін құруды зерттеу қажет. Желілік шабуылдар, істен шығу, желілік құрылғылардың істен шығуы сымсыз желілерде ақпаратты тарату барысында қауіпсіздікке әсер ететін негізгі факторлар болып табылады. Бұл мақалада сымсыз желілерде ақпараттардың қорғалуын қамтамасыз ететін әдістер, соның ішінде аутентификация, шифрлену және қауіпсіздікті қамтамасыз ететін стандарттар қарастырылған. Қауіпсіздіктің бірнеше стандарттары бар, бірақ бұл мақалада сол стандарттардың тиімділігі мен стандарттарда қолданылатын кілттердің жұмыс істеу принциптері айқындалған. Сонымен қатар, мәліметтердің құпиялығы мен тұтастығын қамтамасыз ететін стандарттардың жұмыс істеу қағидасы анықталған. Яғни, TKIP хаттамасы әрбір тасымалданатын мәліметтер пакеті үшін жаңа құпия кілтті генерациялайды және бір статистикалық WEP кілті шамамен 500 миллиард мүмкін болатын кілттерге алмастырылады. Ол осы мәліметтер пакетін шифрлеу үшін қолданылу мүмкін. Кілтті генерациялау механизмі өзгертілген. Ол үш компоненттен тұрады: 128 битті ұзындығы бар базалық кілт(TK), тасымалданатын пакеттің номері(TSC) пен тасымалдаушы құрылғының MAC-адресі(TA). Сонымен қатар, TKIP-те инициализациялаудың 48 разрядты векторы қолданылады. Ол IV векторын қайта-қайта қолдану жағдайын туғызбау үшін қолданылады. TKIP алгоритмі 48 битті ұзындығы бар (TSC) пакет есебін қолданылады. Ол әрдайым артып отырады. Ал, 16 битті TSC жаңа IV енгізіледі(Сурет 4). Осылайша, шабуылдарға тосқауыл бола алатын механизм қалыптасады.

Кілттік сөздер: сымсыз желі, қауіпсіздік, түпнұсқалық, ассиметриялық шифрлеу, меш-портал, стандарт, Cisco Systems, WEP алгоритмі, TKIP хаттамасы, MIC механизмі, IEEE 802.11i стандарты, аутентификация, EAP хаттамалары.

Кіріспе

Ақпараттық технологиялардың дамуы компьютерлік желілердің жұмысының сенімділігін арттыру үшін өзекті міндеттерді алдына қояды. Осындай мәселелерді шешу үшін қолданыстағы желілік хаттамаларды, желі бойынша ақпараттық ресурстарды тасымалдау барысында қауіпсіздікті арттыру үшін тәсілдерді, желінің архитектураларын зерттеу қажет. Сымсыз технологияны таңдау жылдамдық пен ұтқырлықтың артықшылықтарын береді. Кең жолақты сымсыз желілердің(меш-желі) жаңа класының пайда болуы ақпаратты қамту аймағын анағұрлым кеңейтуге мүмкіндік берді. Бұл класстың негізгі артықшылығы арнайы құрылғылардың болуы- меш-желіге басқа да сымсыз желілерді интегрирлеуге мүмкіндік беретін меш—портал мен Интернет. Ал, меш-технологияның кемшілігіне маршрутизация хаттамаларын құру өте күрделі мәселе. Мұндағы қолданылатын хаттамалар қауіпсіздікті сақтау мен арттыру сұрақтары бойынша көптеген қосымша жұмыстарды талап етеді. Желілік шабуылдар, істен шығу, желілік құрылғылардың істемей қалуы ақпаратты тасымалдау барысында қауіпсіздікке әсер ететін негізгі факторлар. Ақпаратты тасымалдау қауіпсіздігін қамтамасыз ету мәселелерімен I. Akyildiz, W. Wang, X. Wang, T. Dorges, N. Ben Salem айналысқан [1].

Scientific Journal of Astana IT University
ISSN (P): 2707-9031
ISSN (E): 2707-904X

Компьютерлік желіде ақпаратты тасымалдаудың қауіпсіздігін қамтамасыз ету деп оның тұтастығын, құпиялығын, қолжетімділігін қорғау болып табылады. Сымсыз желілерде ақпараттардың қолжетімділігін қамтамасыз ету әдістерінің ішіне бақылау, резервтеу, көшірме жасау әдістерін біріктіруді жатқызуға болады. Сымсыз желілерде ақпараттардың тұтастығы мен құпиялығы виртуалды каналдарды құру әдістерімен камтамасыз етіледі. Олар криптографиялық құрал-жабдықтарды қолданумен негізделеді. Бұл әдістердің жалпы кемшілігі болып тасымалданатын ақпараттардың қосымша өңделу талаптарымен сәйкес желілердің өнімдігінің төмендеуі табылады. Бұл кемшілік цифрлы видеоақпаратты тасымалдау барысында байқалады.

Кез келген қолданушы өзінің трафигі үшін үш мәселенің шешілгенін қамтамасыз етуге тырысады: құпиялық(берілген мәліметтер сенімді түрде шифрлену керек), тұтастық(мәліметтер үшінші тұлғамен өзгертілмеу керек), түпнұсқалығы(мәліметтер дұрыс келгені туралы сенімді түрде тексеріс). Осы аталған үш критериялерге тоқталайық.

Түпнұсқалық. Қазіргі таңда сымсыз желілерде 1997-1998 жылдардағы стандарттармен салыстырғанда заманауи түпнұсқалық тәсіл қолданылады. Ол 802.1x стандартында анықталған. Оның принципиалды түрде бастапқы түпнұсқалықтармен салыстырғанда айырмашылығы: өзара тексеріс жүргізілмегенше қолданушы ешқандай мәлімет жібере де ала да алмайды. Стандарт сонымен қатар шифрлену кілттерін динамикалық басқаруды қарастырады. Ал, ол WEP-ке пассивті шабуылды қиындатады. Өңдеушілер қатары өздерінің құрылғыларының түпнұсқасы үшін EAP-TLS пен PEAP хаттамаларын қолданылады. Дегенмен, Cisco Systems өздерінің сымсыз желілері үшін төмендегідей хаттамаларды ұсынады [2]:

- EAP-TLS – IETF стандарты цифрлы сертификаттармен екі жақты алмасу бойынша түпнұсқалықты қамтамасыз етеді;
- PEAP – цифрлы сертификаттармен алмасуды және арнайы құрылған шифрленген туннель бойынша аты мен құпия сөзді қосымша тексеруді қамтамасыз етеді;
- LEAP-екі жақты Challenge Authentification Protokol ұқсас өзара түпнұсқалық хаттамасын ұсынатын Cisco Systems фирмалық хаттамасы. Ол бөлінетін кілт қолданылады, сондықтан да құпия сөздер генерациясы политикасын талап етеді;
- EAP-FAST- сөздік бойынша шабуылдан қорғану үшін IETF стандартының негізінде Cisco-мен өңделген. Оның жұмыс істеу қағидасы LEAP-ке ұқсас, бірақ түпнұсқалық қорғалған туннель бойынша жүргізіледі.

Барлық заманауи түпнұсқаның тәсілдері динамикалық кілттерді қолдаулы білдіреді. Дегенмен, басқа параметрлер бойынша бұл стандарттарды салыстыру қажет болса, онда EAP-TLS мен PEAPауыр болып есептеледі. Олар әр түрлі өндірушілердің құрылғыларының негізінде құрылып бапталған желілерде қолдану үшін жарамды.

Cisco фирмасында құрылған түпнұсқалық тәсілдері тартымдырақ. Оларға бұл тартымдылықты Fast Secure Roaming технологиясы береді. LEAP пен EAP-FAST жұмыс істеу барысында қайта түпнұсқа жүргізу көп уақытты алады. Нәтижесінде хабарлама ажырайды. LEAP пен EAP-FAST хаттамалары Cisco Systems құрылғылары үшін қызмет атқарады.

Шифрлену. Сымсыз желілер үшін әдеттегі сымды желілерге қарағанда қауіпсіздік мәселесі өткір болып табылады, өйткені желінің барлық трафигі радиоарнада алмасады және оны ұстап тұру үшін қымбат емес стандартты жабдық жеткілікті.

Симметриялық шифрлау алгоритмі.

Ақпаратты шифрлеу дегеніміз - ашық ақпаратты шифрланған ақпаратқа айналдыру (көбінесе шифрмәтін немесе криптограмма деп аталады) және керісінше. Бұл процестің бірінші бөлімі шифрлеу деп аталады, ал екінші бөлімі – дешифрлеу [3].

Симметриялық шифрлау алгоритмдерінде шифрлеу және дешифрлеу үшін бірдей кілт немесе қандай да бір қарапайым қатынаспен байланысты кілт қолданылады. Соңғысы, әсіресе қазіргі шифрлеу алгоритмдерінде аз кездеседі. Мұндай кілт әдетте шифрлеу кілті деп аталады. Шифрлеудің келесі формуласын ұсынуға болады:

$$C = E_{k1}(M) \quad (1)$$

M (message) – ашық ақпарат

C (cipher text) – шифрлеу барысында алынған нәтиже;

E (encryption) – M-ге криптографикалық түрлендірулерді орындайтын шифрлеу функциясы.

K_1 (key) – шифрлеу кілті деп аталатын E функциясының параметрі.

28147-89 стандартында кілт түсінігі келесі түрде анықталады: «берілген түрлендіру алгоритмдерінің жиынтығынан бір түрлендіруді қамтамасыз ететін криптографиялық түрлендірудің алгоритмінің кейбір параметрлерінің құпия жағдайы».

Кілт нақты бір қолданушыға немесе қолданушылар тобына жатуы мүмкін. Науқты бір кілтті қолданыла отырып ақпараттың шифрленуі нақты бір қатынаспен байланысты кілтті қолданыла отырып шифрленуі мүмкін.

Ақпаратты дешифрленуді төмендегідей ұсынуға болады:

$$M^{o} = Dk_2(C) \quad (2)$$

M – шифрлеу барысында алынған хабарлама;

D (decryption) – дешифрлеу функциясы;

K_2 – шифрлеу кілті.

Шифрлеу барысында дұрыс ашық мәтінді алу үшін төмендегі шарттарды орындау қажет:

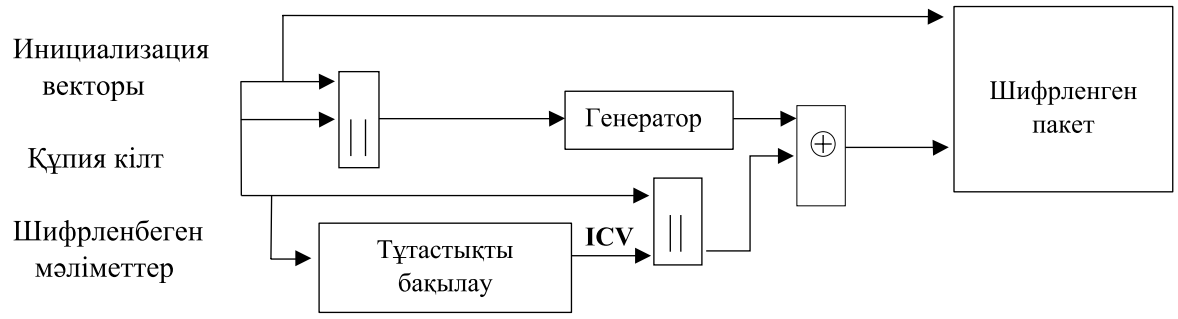
- Дешифрлеу функциясы шифрлеу функциясына сәйкес келу керек;
- Дешифрлеу кілті шифрлеу кілтіне сәйкес келу керек.

Дұрыс k_2 кілт болмаған жағдайда D функциясы көмегімен $M' = M$ ағымдық мәтінді алу мүмкін емес.

WEP қауіпсіздік хаттамасы.

IEEE 802.11(1997 жыл) алғашқы спецификацияда қандай да бір қорғау тәсілі болмады. Дегенмен, SSID идентификатор ашық түрде тасымалданады және оны ұстап алу қиын болмады. Қолжетімділік нүктесінің көбі қалыпты жағдайдағы баптау ретінде Broadcast SSID қолданылады, яғни эфирге ашық түрде желі идентификаторын тасымалдайды.

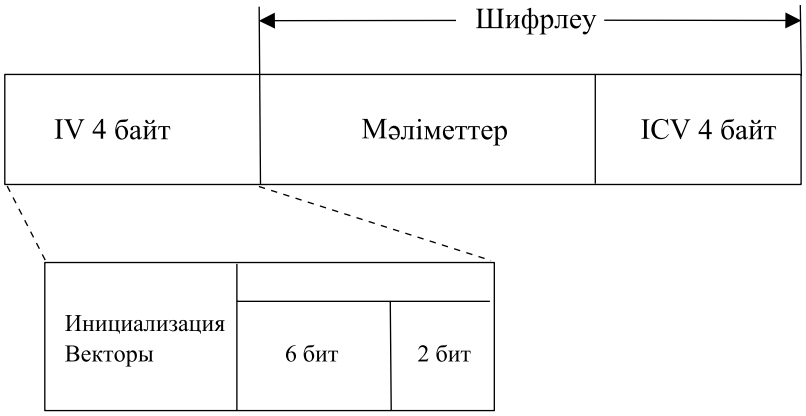
IEEE 802.11-1999 соңғы нұсқасында WEP(Wired Equivalent Privacy) қауіпсіздік хаттамасы енгізілді. Ол IEEE 802.11b құрылғыларында қолданыла бастады.



Сурет 1. WEP (РС-4) хаттамасында мәліметтерді шифрлеу алгоритмі

Scientific Journal of Astana IT University
ISSN (P): 2707-9031
ISSN (E): 2707-904X

WEP алгоритмі бір желіге ұзындығы 40 бит болатын төрт жалпы құпия кілтті қолдануға негізделген. Шифрлеу RC4 компанисының RSA Security алгоритмі бойынша жүзеге асады. Бұл алгоритм шифрленетін мәліметтер блогының ұзындығынддай псевдокездейсоқ реттегі ағымдық мәліметтер блогын көбейтуде қолданылады(Сурет 1). Псевдокездейсоқ реттің генераторы 24 разрядты инициализация векторы(IV — initialization vector) мен 40 разрядты құпия кілттен тұратын 64 разрядты санмен инициализацияланады. Егер де құпия кілт желі құрылғыларына белгілі болса және өзгертілмесе, онда IV вектор пакеттен пакетке өзгеруі мүмкін. Тасымалданатын ақпараттың рұқсатсыз өзгеруінен қорғану үшін әрбір шифрленген пакет 32 разрядты бақылау CRC-32 қосындысымен қорғалады. Демек, шифрлеу барысында тасымалданатын мәліметтерге 8 байт қосылады: 4 байт ICV үшін, 3 байт IV үшін, ал 1 байт құпия кілттің номері туралы ақпараттан тұрады(Сурет 2). Кілт 64 байт ғана емес, 128 байтта болуы мүмкін.



Сурет 2. WEP-шифрлеуден кейінгі пакет

RC4 алгоритмі симметриялы болып табылады, яғни шифрлеу мен дешифрлеу үшін бір кілт қолданылады. Ол жоғары жылдамдықты жұмысты, бірақ төменгі криптотұрақтылықты қамтамасыз етеді. WEP алгоритмі жалпы төменгі криптотұрақтылыққа ие. 64 битті ұзындығы бар кілт бірнеше секунд ішінде таңдап алу әдісі бойынша жинақталады. Ал, 128 битті кілт үшін көбірек уақыт қажет, бірақ FMS шабуылдың пайда болуынан бастап таңдау алу алгоритмі қолданылмайтын болды. FMS шабуылдар RC4 кілттерді тағайындау барысында әлсіз жақтарды қолданылады. Соның негізінде парольді бұзу үшін 6 млн. пакет жинақталады. Қарапайым желілер үшін ол пакет саны көп, сондықтан да шабуыл жасау үшін бірнеше сағаттан бірнеше тәулікке дейін созылуы мүмкін. DasbOden Labs лабораториясының қызметкерлері пакеттерді бұзу үшін 500 мыңға дейін қысқартты.

2004 жылдың тамыз айында KoreK хакер 200 және 500 мың пакеттерді қолданыла отырып, 40 пен 104 битті кілттерді бұза алатындай статистикалық криптоталдауды жазды. Оның алгоритмі қазіргі таңда WEP кілттерін бұзу үшін негізгі құрал болып табылатын aircrackутилитасында қолданылды.

Сонымен қатар, WEP хаттамасы түпнұсқалық функциясын атқарады. Дегенмен оны толыққанды деп атауға болмайды, себебі қолданушы қолданған құпия сөзге негізделген. Бұл мәселені MAC-адрестердің тізімін қолданумен шешуге тырысты, бірақ MAC-адрестер ашық түрде тасымалданады. Сонымдқтан да олар жол ортадан алынып, өзгертілуі мүмкін.

WEP хаттамада түпнұсқалықтың екінші мәселесі болып оның біркелкілігі табылады, яғни кіру нүктесінің заңдылығын анықтай алмайтын клиент құрылғыларын ғана аутентификациялайды. Бұл мәселені шифрлеу кілтінің ұзындығын арттыру арқылы шешілді, бірақ желінің өткізу қабілеті төмендеді. Сондықтан да өндірушілер бұл алгоритмді жаңартпады.

WEP хаттама- шифрлеу үрдісі: бұл хаттама желі бойынша мәліметтерді тасымалдау барысында мәліметтерді қорғауды қамтамасыз ету керек. Оның негізінде арнайы кілттің көмегімен тасымалданатын пакеттерді шифрлеу жатыр. Шифрлеу үрдісін қарастырайық[4].

Қорытынды бақылау: бірінші деңгей. (M) хабарламаның бақылау суммасы есептеледі. Содан кейін бақылау суммасы хабарламаның өзіне қосылады: P = (M, c(M)). Ол екінші деңгейдің ағымдық мәліметі болып табылады. Шифрлеудің екінші деңгейінде P мәтіні RC4 алгоритмі бойынша шифрленеді. Бастапқы вектор (IV) болсын. RC4 алгоритм keystream-ді генерациялайды, яғни IV пен k кілтке тәуелді кездейсоқ байттардың реті. Бұл keystream-ді RC4(v,k) ретінде анықтайық. XOR әдісі бойынша забарлама keystream-ға қабаттасады да шифрленген хабарламаны аламыз:

$$C = P \text{ xor } RC4(v,k).$$

Тасымалдау: соңғы деңгей. IV мен желі бойынша шифрленген хабарлама тасымалданады.

Оның барлығын мынадай түрде келтіруге болады:

$$A - B: v, (P \text{ xor } RC4 (v, k)), \text{ мұндағы } P = (M, c (M)).$$

Келесі қысқартуларды келесі қолдануларға енгіземіз: (M) хабарламасы – шифрлеуге арналған ағымдық мәліметтер; (P) мәтіні- хабарлама суммасы мен оның бақылау суммасы; (C) пакет – желі бойынша таратылатын шифрленген мәтін.

Алынған мәліметтерді дешифрлеу үшін хабарламаны алушы кері қызметтерді орындайды. Біріншіден, keystream RC4(v,k) генерацияланады және XOR амалының көмегімен пакетті мәтінге түрлендіреді.

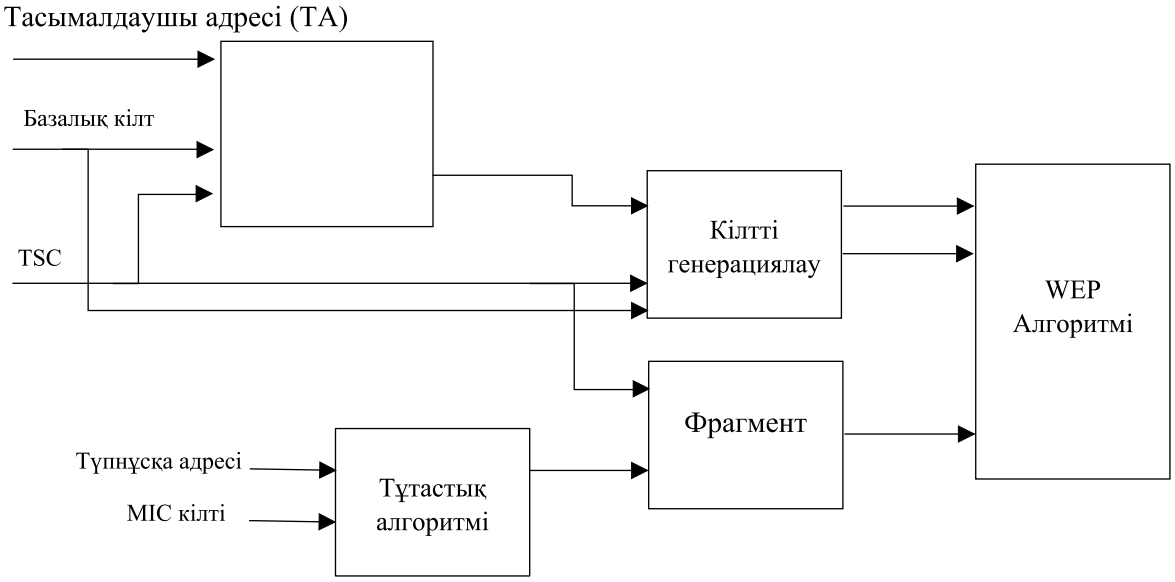
$$P' = C \text{ xor } RC4(v,k) = (P \text{ xor } RC4(v,k)) \text{ xor } RC4(v,k) = P.$$

Алушы P' декодталған мәтіннің бақылау суммасын тексереді де алынған C' сәйкестігін тексереді. Демек, қолданушы дұрыс бақылау суммасы бар пакеттерді ғана алатынын біледіреді.

WPA стандарты. WPA (Wi-Fi Protected Access) стандарты 2004 жылы қабылданған IEEE 802.11i стандартынан сипаттамаларды ұсынады. WPA стандартының сипаттамасы WEP үшін қолданушыларға ұқсастықты ұсынды және олар мен жаңа IEEE 802.11i стандарты арасында өтпелі баспалдақ ретінде қолданылды. WPA құрылымын мынадай формула түрінде ұсынуға болады: WPA = IEEE 802.1X + EAP + TKIP + MIC, яғни WPA бірнеше элементтердің суммасы болып табылады[5].

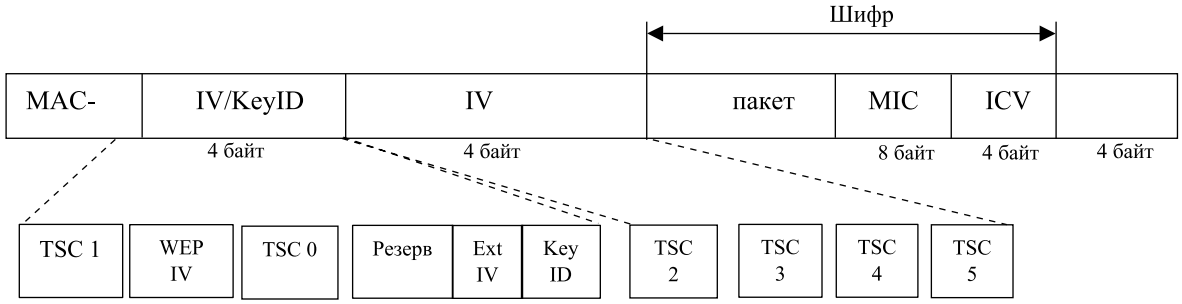
IEEE 802.1X пен EAP (Extensible Authentication Protocol) хаттамалары желіге қолжетімділік үшін куәлікті ұсыну қажет болатын қолданушылардың аутентификация механизмін қамтамасыз етеді. Көлемді корпоративті желілерді түпнұсқалық үшін RADIUS серверін қолданылады. Желі иерархиясында ол кіру нүктесінен жоғары тұрады және қолданушылар тізімін қамтитын мәліметтер қорынан тұрды. Желілік қауіпсіздіктің мұндай жүйесі Enterprise(корпоративті) деп аталады. Кішігірім фирмалар мен үй қолданушылары үшін алдын ала тағайындалған PSK (Preshared Key)кілті бар режим қарастырылған. Бұлл режимде сымсыз желінің әрбір құрылғысына біркелкі құпия сөз бен аутентификация енгізіледі.

Scientific Journal of Astana IT University
ISSN (P): 2707-9031
ISSN (E): 2707-904X



Сурет 3. TKIP хаттамасы бойынша шифрлеу

TKIP (Temporal Key Integrity Protocol) – уақытша тұтастық хаттамасы) хаттамасы мәліметтердің құпиялығы мен тұтастығын қамтамасыз етеді. TKIP функционалды түрде WEP кеңейтілімі болып табылады (Сурет 3). WEP хаттамасы на ұқсас RC-4 шифрлеу алгоритмін қолданылады, бірақ кілттерді басқару механизмі анағұрлым тиімді. TKIP хаттамасы әрбір тасымалданатын мәліметтер пакеті үшін жаңа құпия кілтті генерациялайды және бір статистикалық WEP кілті шамамен 500 миллиард мүмкін болатын кілттерге алмастырылады. Ол осы мәліметтер пакетін шифрлеу үшін қолданылу мүмкін. Кілтті генерациялау механизмі өзгертілген. Ол үш компоненттен тұрады: 128 битті ұзындығы бар базалық кілт (ТК), тасымалданатын пакеттің номері (TSC) пен тасымалдаушы құрылғының MAC-адресі (ТА). Сонымен қатар, TKIP-те инициализациялаудың 48 разрядты векторы қолданылады. Ол IV векторын қайта-қайта қолдану жағдайын туғызбау үшін қолданылады. TKIP алгоритмі 48 битті ұзындығы бар (TSC) пакет есебін қолданылады. Ол әрдайым артып отырады. Ал, 16 битті TSC жаңа IV енгізіледі (Сурет 4). Осылайша, шабуылдарға тосқауыл бола алатын механизм қалыптасады.



Сурет 4. TKIP бойынша шифрлеуден кейінгі пакет

Ойнатылымы бар шабуылдар бұзуды жылдамдату үшін арнайы құрал-жабдықтарды пайдаланады немесе сымсыз хосттардың порттарын сканерлейді. WEP шеңберінде мұндай шабуылдарды тоқтату мүмкін емес. Көп жағдайда таңдау кездейсоқ түрде жүзеге асырылады.

MIC (Message Integrity Check немесе Michael) механизмін қарастырайық. Ол хабарламалардың тұтастығын тексеруді қамтамасыз етеді. Бұл механизм CRC-32 негізінде құрылады,

бірақ MIC ұзындығы 64 битке тең. ICV қарағанда MIC механизмі қуатты хэш-функцияны қолданылады. Бұл функцияны жіберуші мен алушы қолданылады. Нәтижесінде қорытындыны салыстырады. Егер де ол сәйкес келмейтін болса, онда мәліметтер жалған болып табылып пакеттер лақтырылады. Сонымен қатар, алгоритмге шабуалға қарсы тосқауылдар енгізілген. Егер де қабылдаушы 60 с ішінде MIC-та екі қате табатын болса, онда байланыс үзіледі де 60 с қайта қалпына келтіріледі. 2008 жылы TKIP хаттамасына шабуыл алгоритмі сипатталды. Криптоқорғаудың деңгейін арттыру үшін IEEE 802.11i (WEP2) стандарты қолданылды. Барлық жаңашылдыққа қарамастан WPA бұрынғы IEEE 802.Ha/b/g сипаттамалармен сәйкес келе береді және оны қолдану үшін оның драйверін ғана жаңарту қажет. Жаңа IEEE 802.11i стандартты қолдану үшін жаңа құрылғы қажет, себебі RC4 шифрлеудің орнына AES стандарты келді.

IEEE 802.11i стандартының архитектурасы. 2004 жылы қабылданған IEEE 802.11i стандарты WPA-мен ұқсас келеді, бірақ қауіпсіздіктің жоғары деңгейін ұсынады. IEEE 802.11i стандартында сенімді түрде қорғалған желінің концепциясы анықталған- Robust Security Network (RSN). Бұл стандарт AES (Advanced Encryption Standard) стандартының блокты шифрының негізінде CCMP (Counter-Mode CBC MAC Protocol) хаттамасын ұсынады. CCMP хаттамасы үшін AES алгоритмі RC4 сияқты роль атқарады. Екі хаттамада да кілтті басқарудың бір механизмімен жұмыс істейді. TKIP сияқты CCMP 48-битті IV пен кішігірім өзгерісі бар MIC қолданылады. AES қолданудың негізінде пакетті кілттерді генерациялау қажеттілі жоқ. Сервер мен клиенттің ассоциасы кезінде құрылған кілт трафикті шифрлеу мен бақылау суммасын генерациялау үшін қолданылады[6].

IEEE 802.11i аутентификация үрдісінің үш қатысушысын қарастырады: аутентификация сервері(Authentication Server, AS), кіру нүктесі(Access Point, AP), жұмыс станциясы(Station, STA). Мәліметтерді шифрлеу процесі барысында AP мен STA ғана қолданылады.

Бұл стандарт екі жақты аутентификацияны қарастырады. Қолжетімділікке рұқсат туралы шешімді қабылдау STA пен AS, ал ал ол шешімді орындау STA мен AP табылады. IEEE 802.11i стандарты бойынша жұмыс істеу үшін Master Key (MK), Pairwise Master Key (PMK), Pairwise Transient Key (PTK), GTK кілттер тобынан тұратын кілттер иерархиясы құрылады. Мұндағы [7]:

MK – өазара аутентификация туралы STA мен AS шешімдерін жүзеге асыратын симметриялы кілт. Әрбір жаңа сессия үшін жаңа MK кілті құрылады;

PMK – берілген сессияда мәліметтерді тасымалдау үшін қолжетімділікті рұқсат етуді білдіретін жаңартылып отыратын симметриялы кілт; PMK MK негізінде құрылады. STA мен AP әрбір жұбы үшін жаңа PMK кілті құрылады;

PTK – PMK-ны STA мен AP мәліметтеріне біріктіру үшін қолданылатын операционды кілттер жиынтығы.

IEEE 802.11i стандартының жұмыс істеуінің бес фазасы бар:

Табу фазасында STA AP-ны табады да байланыс орнатады. Содан кейін желіде қолданылатын қауіпсіз параметрлерін алады. Осылайша STA желінің (SSID) идентификаторын және аутентификация әдісін анықтайды. Келесі қадам ретінде STA аутентификация әдісін таңдайды да STA мен AP арасында байланыс орнатады.

IEEE 802. IX аутентификация фазасында STA мен AS өзара аутентификациясы орындалады, MK мен PMK құрылады. Бұл фазада STA мен AP IEEE 802.IX-дан басқа барлық трафиктерді блоктайды.

Үшінші фазада AS PMK-ны кіру нүктесіне орналастырады. Енді STA мен AP PMK-ң нақты кілттеріне ие болады.

Төртінші фаза – IEEE 802.IX кілттерін басқару. Бұл фазада PTK кілтін генерациялау, байланыстыру, верификация орындалады.

Scientific Journal of Astana IT University
ISSN (P): 2707-9031
ISSN (E): 2707-904X

Бесінші фаза – мәліметтерді шифрлеу мен тасымалдау. Шифрлеу үшін РТК-ң сәйкес бөлігі қолданылады.

Кілттердің аутентификациясы мен жеткізілуі IEEE 802.IX стандартымен анықталады. Ол сымсыз желілерде аутентификацияның дәстүрлі серверлерін қолдану мүмкіндігін ұсынады. IEEE 802.11i сипаттамасы аутентификацияның сервер типін анықтамайды, бірақ стандартты сервер RADIUS (Remote Authentication Dial-In User Server) болып табылады.

IEEE 802.11i Pre-Shared Key (PSK) режимін қолдануды қарастырады. Бұл режимді қолдану барысында STA мен AP-ға Pre-Shared Key кілті өздігінен енгізіледі. PSK режимі кішігірім желілерде қолданылады.

IEEE 802. IX хаттамасы. Бастапқыда IEEE 802.IX стандарты 2 деңгейдегі қолданушылардың аутентификациясын қамтамасыз ету үшін ойластырылған. Сымсыз жергілікті желіде IEEE 802.IX стандарты қосымша функцияға ие: кілттерді динамикалық тағайындау. Оны қолдау үшін кілттердің екі жиынтығы генерацияланады. Бірінші жиынтық клиент хосты мен кіру нүктесі арасында әмбебап байланысты орнату үшін сеансты кілттерден тұрады. Сеансты кілттер каналдардың құпиялығын қамтамасыз етеді.

Екінші жиынтық кілттер тобынан тұрады. Топтық кілттер IEEE 802.11 желісінде бір соттағы барлық хосттар бойынша бөлінеді және топқа арналған трафикті шифрлеу үшін қолданылады. Сеансты және жұпты кілттердің ұзындығы 128 битті құрайды. Жұптық кілттер ұзындығы 256 бит болатын негізгі жұптық кілттерден тарайды. РМК желінің әрбір құрылғылысына RADIUS-сервермен беріледі. Топтық кілттер Groupwise Master Key — GMK негізгі топтық кілттен тарайды. RADIUS серверін соңғы пайдаланушының дерекқорымен жиі пайдалану мүмкін емес.

Демек, сеансты кілттерді генерациялау үшін алдын ала тағайындалған РМК кілті қолданылады. Жергілікті IEEE 802.11 желілерде физикалық порттар болмағандықтан, сымсыз клиент құрылғылар мен кіру нүктесі арасында ассоциация қолжетімділіктің желілік порты болып есептеледі. Сымсыз клиент үміткер ретінде, ал кіру нүктесі аутентификатор ретінде қарастырылады. Демек, IEEE 802.IX стандартының терминологиясында кіру нүктесі Ethernet сымды желілердің коммутатор ролін атқарады. Яғни, кіру нүктесіне қосылған желінің сымды сегменті аутентификация серверін қажет етеді. Әдетте оның функциясын RADIUS-сервер атқарады. Жоғары класстың коммерциялық сымсыз шлюздері аутентификацияның сервер функциясы ретінде жүзеге асырылады.

IEEE 802.IX стандартында 2 деңгейдің қолданушылар аутентификациясы EAP (Extensible Authentication Protocol) хаттамасы бойынша орындалады. EAP хаттамасы ол CHAP әдісінің ауыстырылуы. Ол «нүкте-нүкте» хаттамасында қолданылады.

Аутентификацияның орындалу қағидасын қарастырайық. Канал орнатылғаннан кейін аутентификатор идентификацияның басқапты сұранысын тасымалдайды. Үміткер әрбір сұранысқа жаңап қайтарады. Аутентификатор әрбір аутентификация үрдісін аутентификацияның орындалғаны немесе орындалмағаны туралы хабарламаны жібергеннен соң аяқтайды. EAP хабарламасының құрылымы RADIUS пакетінің құрылымымен ұқсас.

EAP хаттамаларының бірнеше нұсқалары бар [8].

EAP-MD5- IEEE 802.IX стандартының барлық қызметтерінде болу керер EAP-тың міндетті деңгейі. Функционалды түрде ой CHAP хаттамасын қайталайды. EAP-MD5 хаттамасын үш себеп бойынша қолдануды ұсынбайды. EAP-MD5 кілттердің динамикалық тағайындалуын орындамайды. «Адам ортасында» шабуылы үшін және аутентификация серверіне шабуылға осал болып табылады. Аутентификация барысында қарсылас сұранысты және шифрленген жауапты білуі мүмкін.

EAP-TLS (Transport Layer Security, RFC 2716) сертификаттар базасында өзара аутентификацияны қолдайды. EAP-TLS SSLv3 хаттамасы бойынша негізделген.

EAP-LEAP (Lightweight EAP или EAP-Cisco Wireless) – бұл Cisco компаниясымен патенттелген EAP нұсқасы. LEAP IEEE 802.IX стандартында аутентификацияның алғашқы сызбасы болды.

EAP ішінде ең аз тараған PEAP (Protected EAP, IETF) пен EAP-TTLS (Tunneled Transport Layer Security EAP). EAP-TTLS-пен жұмыс істеу үшін аутентификацияның сервері ғана сертификатталған болуы талап етіледі. EAP-TTLS аутентификацияның ескі PAP, CHAP, MS-CHAP, MS-CHAPv2 и EAP-MD5 сияқты әдістерін де қолдайды

Қорытындылай келе сымсыз желілерде ақпараттарды қорғау әдістерінің жоғары деңгейін WPA мен 802.11i стандарттары қамтамасыз етеді. Дегенмен, қауіпсіздік үшін қорғаудың бір хаттамасы жеткіліксіз, сонымен қатар желі дұрыс баптау мен құру қажет.

Физикалық қорғау. Wi-Fi-желісін орналастырған кезде сымсыз нүктелерге қолжетімділікті физикалық шектеу қажет.

Дұрыс баптау. Заманауи сымсыз желілердегі қарама-қайшылық – қолданушылар аутентификация мен шифрлеудің енгізілген механизмдерін қоспайды және қолданбайды.

Қолданушылық құрылғыларды қорғау. Желінің енгізілген қорғау механизмдеріне толық сенбеу қажет. Ең оңтайлы - тереңдетілген қорғаныс әдісі, оның бірінші желісі тұрақты компьютерде, ноутбукта немесе PDA-де орнатылған қорғаныс құралдары болып табылады.

Дәстүрлі әдістер. Желіде компьютердің тиімді жұмысы классикалық қорғау әдістерінсіз мүмкін емес, яғни уақтылы жаңартуларды орнату, қорғау механизмдерін қолдану.

Желіге мониторинг жүргізу. Корпоративтік желідегі әлсіз байланыс - бұл рұқсат етілмеген кіру нүктелері. Рұқсат етілмеген кіру нүктелерін оқшаулау мәселесі өзекті болып табылады. Кіру нүктелерін локализациялаудың арнайы құралдары қабаттың немесе ғимараттың картасында «бөтен» терминалдың орналасқан жерін графикалық түрде көрсетуге мүмкіндік береді. Егер классикалық әдістер сізді басып кіруден сақтамаса, шабуылды анықтау жүйелерін қолдану керек.

VPN-агенттер. Көптеген кіру нүктелері ашық режимде жұмыс істейді, сондықтан да тасымалданаттын мәліметтерді қорғау әдістерін қолдану керек. VPN клиенті осы тапсырманы орындау үшін қорғалатын компьютерге орнатылуы керек. Барлық заманауи операциялық жүйелерде осындай бағдарламалық компоненттер бар.

Әдебиеттер тізімі

1. Вишневский В.М., Портной С.Л., Шахнович И.В. “Энциклопедия WiMAX. Путь к 4G”. Москва: Техносфера, 2009 г.
2. Шахнович И.В. “Современные технологии беспроводной связи”. Издание второе, исправленное и дополненное. Москва: Техносфера, 2006 г.
3. “Системы мобильной связи”. Учебное пособие для вузов / В.П. Ипатов, В.К. Орлов, И.М. Самойлов, В.Н. Смирнов, под ред. В.П. Ипатова.
4. Барнс К. Защита от хакеров беспроводных сетей / К. Барнс, Т. Боутс, Д. Лойд. М.: ДМК-Пресс, 2005. – 480 с.
5. Вишневский В.М. Широкополосные беспроводные сети передачи информации / В.М. Вишневский, А.И. Ляхов, С.Л. Портной, И.Л. Шахович. М.: Техносфера, 2005. – 592 с.
6. Ю. Вишневский В. Mesh-сеrа стандарта IEEE 802.11s – технологии иреализация / В. Вишневский, Д. Лаконцев, А. Сафонов, С. Шпилев // Первая миля. – 2008. – №2.
7. Владимиров А.А. Wi-фу: «боевые» приемы взлома и защиты беспроводных сетей / А.А. Владимиров, К.В. Гавриленко, А.А. Михайловский. – М.: НТ Пресс, 2005. – 464 с.
8. Романец Ю.В. Защита информации в компьютерных системах и сетях / Ю.В. Романец, П.А. Тимофеев, В.Ф. Шаньгин. – М.: Радио и связь, 2001. – 376 с.

Scientific Journal of Astana IT University
ISSN (P): 2707-9031
ISSN (E): 2707-904X

Reference

1. Vishnevskij V.M, Portnoj S.L. & Shahnovich I.V. “Enciklopedija WiMAX. Put’ k 4G”. Moskva: Tehnosfera, 2009.
2. Shahnovich I.V. “Sovremennye tehnologii besprovodnoj svjazi”. Izdanie vtoroe, ispravlennoe i dopolnennoe. Moskva: Tehnosfera, 2006.
3. “Sistemy mobil’noj svjazi”. Uchebnoe posobie dlja vuzov / V.P. Ipatov, V.K. Orlov, I.M. Samojlov & V.N.Smirnov. pod red. V.P. Ipatova.
4. Barns K. Zashhita ot hakerov besprovodnyh setej / K. Barns, T. Bouts. & D. Lojd. – M.: DMK-Press, 2005. – 480 p.
5. Vishnevskij V.M. Shirokopolosnye besprovodnye seti peredachi informacii / V.M. Vishnevskij, A.I. Ljahov, S.L. Portnoj, I.L. & Shahovich. – M.: Tehnosfera, 2005. – 592 p.
6. Yu. Vishnevskij V. Mesh-cera standarta IEEE 802.11s – tehnologii irealizacija / V. Vishnevskij, D. Lakoncev, A. Safonov & S. Shpilev // Pervaja milja. – 2008. – №2.
7. Vladimirov A.A. Wi-fu: «boevye» priemy vzloma i zashhity besprovodnyh setej / A.A. Vladimirov, K.V. Gavrilenko. & A.A. Mihajlovskij. – M.: NT Press, 2005. – 464 p.
8. Romanec Ju.V. Zashhita informacii v komp’juternyh sistemah i setjah / Yu.V. Romanec, P.A. Timofeev. & V.F. Shan’gin. – M.: Radio i svjaz’, 2001. – 376 p.

Главный редактор:
Белощицкий А.А.
Ответственный редактор:
Амиргалиев Б.Е.

Подписано в печать 29.04.2020 г.
Формат 60х84 1/8. Усл. п.л 14.
Тираж 300 экз. Заказ №67.
Отпечатано в ТОО «Шаңырақ-Медиа».
г. Нур-Султан, ул. Кокарал, 2/1, тел. 87077770066.
www.smedia.kz