ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ
«АЛМАТЫ ЭНЕРГЕТИКА ЖӘНЕ БАЙЛАНЫС УНИВЕРСИТЕТІ»
коммерциялық емес акционерлік қоғамы
«Ақпараттық қауіпсіздік жүйелері» кафедрасы

«ҚОРҒАУҒА ЖІБЕРІЛДІ»
Кафедра меңгерушісі с.ғ.к., доцент Бердібаев Р. Ш.
_____ «_____» _____ 2019 ж.
(қолы)

ДИПЛОМДЫҚ ЖОБА

Тақырыбы: «TLS хаттамасының қауіпсіздігін зерттеу»
Мамандығы: 5В100200 – «Ақпараттық қауіпсіздік жүйелері»
Орындаған: Шакирова Бақыт Тобы: СИБк-15-1
Ғылыми жетекші: т.ғ.к., доцент Омар Т.К.

Кеңесшілер:
Экономикалық бөлім бойынша:
э.ғ.к., профессор Әренбаева Қ.Г.
(ғылыми дәрежесі, атағы, аты-жөні)
_____ «13» 05 2019 ж.
(қолы)

Тіршілік қауіпсіздігі бөлімі бойынша:
аға оқытушы Торғаев Э.Э.
(ғылыми дәрежесі, атағы, аты-жөні)
_____ «27» 05 2019 ж.
(қолы)

Есептеу техникасын қолдану бойынша:
Омар Т.К.
(ғылыми дәрежесі, атағы, аты-жөні)
_____ «20» 05 2019 ж.
(қолы)

Мөлшер бақылаушы:
аға оқытушы, т.ғ.м., Асқарова Н.Б.
(ғылыми дәрежесі, атағы, аты-жөні)
_____ «31» 05 2019 ж.
(қолы)

Пікір беруші: PhD Шаяхметова А.С.
(ғылыми дәрежесі, атағы, аты-жөні)
_____ «03» 06 2019 ж.
(қолы)

Алматы 2019

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ
«АЛМАТЫ ЭНЕРГЕТИКА ЖӘНЕ БАЙЛАНЫС УНИВЕРСИТЕТІ»
коммерциялық емес акционерлік қоғамы

Басқару және ақпараттық технологиялар институты
Ақпараттық қауіпсіздік жүйелері кафедрасы
5В100200 – «Ақпараттық қауіпсіздік жүйелері» мамандығы

Дипломдық жобаны орындауға берілген
ТАПСЫРМА

Студент: Шакирова Бақыт
(аты-жөні)

Жобаның тақырыбы: „TLS хаттамасының қауіпсіздігін" зерттеу

2018 ж. «26» 10 №124 универститет бұйрығымен бекітілді.

Аяқталған жұмысты тапсыру мерзімі: «____»______________20___ ж.

Жобаға алғашқы деректер (талап етілетін зерттеу (жоба) нәтижелерінің параметрлері және зерттеу нысанының алғашқы деректері): Құпия ақпаратты беру кезінде клиент пен сервер арасында қауіпсіз байланыс орнату үшін қолданылатын TLS хаттамасының осалдығын зерттеу. SSL/TLS криптографиялық хаттамасының негізгі осалдықтарына талдау жүргізу, сондай-ақ OpenSSL көмегімен осы осалдықтардың бар болуына TLS зерттеу процедураларын келтіру. Клиент-сервер байланысының қорғалуын бағалау үшін жүргізілетін тексерудің толық болуына және TLS сынақтарының қауіпсіздігін тестілеу әдістемесін ұсыну.

Диплом жобасындағы әзірленуі тиіс мәселелер тізімі немесе диплом жобасының қысқаша мазмұны:
1. SSL/TLS хаттамасы арқылы ақпаратты қауіпсіз жіберуді қамтамасыз ету;
2. TLS хаттамасының белгілі осалдықтары мен шабуылдарын зерттеу;
3. Талдау әдістемесін қалыптастыру;
4. Талдау нәтижелерін келтіру;
5. Техникалық-экономикалық негіздеме;

6. Өндірушілік қауіпсіздігі;
7. Қорытынды

Графикалық материалдардың (міндетті түрде дайындалатын сызбаларды көрсету) тізімі:

1. OSI моделіндегі TLS хаттамасының орны көрсетілген сызба;
2. Қол алысу кезеңінің схемасы;
3. Хаттама құрылымының мысалы;
4. Шабуылдардың жүзеге асыру схемасы;
5. OpenSSL ұдайы таңдау нәтижелері;

Негізгі ұсынылатын әдебиеттер:

1. Сланов Ю. Т., „Алгоритмы телекоммуникационных сетей". 2004 Т31. 126-2076.
2. Ivan Ristic. „Bulletproof SSL and TLS", 2014.
3. Брюс Шнайер „Прикладная криптография" 1994, №2, 91-99б.

Жоба бойынша жобаның бөлімдеріне қатысты белгіленген кеңесшілер

Бөлімдері	Кеңесшілері	Мерзімі	Қолы
	Омар Б. К	04.03-20.05	
	Тораев Ә.Ғ.	18.03-27.05	
	Арепбаева Ж.Т.	04.03-13.05.19	

Диплом жобасын дайындау
КЕСТЕСІ

Бөлімдердің атауы, әзірленетін мәселелердің тізімі	Ғылыми жетекшіге ұсыну мерзімдері	Ескерту
1. SSL/TLS хаттамасы арқылы ақпаратты қауіпсіз жіберуді қамтамасыз ету.	15.02.2019	
2. TLS хаттамасы арқылы белгілі осалдықтарды мен шабуылдарын зерттеу	29.02.2019	
3. Талдау әдістемесін қалыптастыру	07.03.2019	
4. Талдау нәтижелерін енгізу	15.03.2019	
5. Өміртіршілік қауіпсіздігі	02.04.2019	
6. Техникалық-экономикалық негіздеме	29.04.2019	
7. Қорытынды	20.05.2019	

Тапсырманың берілген уақыты «_____» _____ 20___ж.

Кафедра меңгерушісі _____ (_____)
(колы) (аты-жөні)

Жобаның
ғылыми жетекшісі _____ (Омар Ә.К.)
(колы) (аты-жөні)

Орындалатын тапсырманы
қабылдаған студент _____ (Шакирова Б.Т.)
(колы) (аты-жөні)

АҢДАТПА

Осы дипломдық жұмыс TLS хаттамасын жүзеге асырудың қауіпсіздігі мәселесіне арналған және TLS протоколын іске асырудың тестілеу әдістемесін әзірлеуге бағытталған. Жұмыс барысында хаттамаға шабуылдар талданды, параметрлер бөлінді, олардың көмегімен шабуылдар іске асырылды. Хаттаманың TLSv1.0, TLSv1.1, TLSv1.2 нұсқалары сыналған тестілеу әдісі жасалды. Тестілеу нәтижелері мен қорғау бойынша ұсыныстар келтірілді.

АННОТАЦИЯ

Настоящая диломная работа посвящена вопросу безопасности реализаций протокола TLS и направлена на разработку методики тестирования реализации прокола TLS. В ходе работы были проанализированы атаки на протокол, выделены параметры, с помощью которых атаки были реализованы. Была создана методика тестирования, по которой были протестированы протоколы версий TLSv1.0, TLSv1.1, TLSv1.2. Приведены результаты тестирования и рекомендации по зпщите.

ANNOTATION

This thesis is devoted to the issue of security implementations of the TLS Protocol and is imed at developing a methodology for testing the implementation of the TLS Protocol. In the course of the work, the attacks on the Protocol were analyzed, the parameters by which the attacks were implemented were highlighted. Was created testing methodology, which was tested protocols versions TLSv1.0, TLSv1.1, TLSv1.2. The results of testing and recommendations for protection are given.

Мазмұны

Кіріспе

SSL/TLS хаттамасы және дейтаграмм режимінде жұмыс істейтін DTLS нұсқасы HTTP, SMTP, IMAP, POP, SIP және XMPP сияқты қосымшалар деңгейіндегі хаттамалардың деректерімен алмасуды қорғау үшін кеңінен қолданылады. Соңғы бірнеше жылда TLS хаттамасына бірнеше маңызды шабуылдар пайда болды, олардың кейбіреулері жиі қолданылатын криптоалгоритмдер жиынтығына бағытталған. Мысалы, өткен танымал AES-CBC және RC4 шифрлау алгоритмдерінің екеуі де TLS контекстінде шабуыл болды.

Хаттаманың бірінші нұсқалары 20 жыл бұрын жасалды. Осы уақыт ішінде зерттеушілер SSL 2.0 және 3.0 архитектурасында көптеген осалдықтарды тапты, сәтті шабуылдарды іске асырды. Сондықтан бұл нұсқалар мен TLS хаттамасынан SSL-ға дейінгі төмендеілген кейбір механизмдері қауіпсіз емес деп танылды.

TLS хаттамасы көптеген криптографиялық алгоритмдер мен кеңейтулерді қолдайды, демек, іске асыру өте қиын болып табылады. Бірақ бұл әзірлеушілерді тоқтатпайды: хаттама ашық және жабық бастапқы коды бар көп іске асыру санымен ұсынылған. Хаттамаға кейбір елеулі шабуылдар оны іске асырудағы қателіктерге байланысты.

Хаттамада пайда болған шабуылдардың себебі бойынша хаттаманың конфигурациялық параметрлерін тестілеу әдістемесін әзірлеу, хаттаманы пайдаланатын клиенттік және серверлік веб-қосымшалар үшін әдістемені іске асыру, қорғау бойынша ұсыныстарды қалыптастыру және қолдану өзекті мәселе болып отыр.

Қолданыстағы хаттама қауіпсіздігінің зерттеулері артық теориялық сипатқа ие және пайдаланушылардың қорғалуын тестілеу мәселелерін шешуді ұсынбайды. Пайдаланушыларды тестілеу бойынша әзірленген шешімдер жеткілікті түрде аз, олардың негізгі проблемаларына ұсынылған тексерулердің толықтығы мен хаттаманың қорғалған параметрлерін таңдау бойынша ұсыныстарды қалыптастыру мен қолдану кезеңінің болмауын жатқызуға болады. Нәтижесінде хаттамалардың қауіпсіздігін тестілеудің толық әдістемесін жасау үшін қадамдар жасалды.

1 SSL/TLS хаттамасы арқылы ақпаратты қауіпсіз жіберуді қамтамасыз ету

1.1 OSI моделіндегі SSL/TLS хаттамасының орны

Қазіргі заманғы компьютерлік техниканың даму кезеңінде кез-келген операциялық жүйе үшін стандарты жағдай желілік функциялардың болуы болып табылады. ОЖ желілік мүмкіндіктері клиенттің көптеген танымал web-қосымшаларды және жалпы Интернетті пайдалануын қамтамасыз етеді. Желі бойынша ақпаратты беру үшін 1978 жылы стандарттау жөніндегі халықаралық ұйым (ISO) әзірлеген ашық жүйелердің өзара іс-қимылының базалық моделі (OSI) іргетасы болып табылатын әртүрлі желілік хаттамалар қолданылады. OSI моделінде жіберілетін деректердің қауіпсіздігіне байланысты мәселелерге ерекше көңіл бөлінген. ISO 7498-2 стандарты жеті үлгінің әрқайсысында ақпаратты қорғауға арналған қызметтер мен қорғау механизмдерінің тізбесін анықтайды. Қызмет ұғымы дерексіз және қауіпсіздік талаптарын анықтауға арналған. Өз кезегінде қауіпсіздік механизмдері қызметтерді іске асырудың нақты шаралары болып табылады.

Алмасуға қатысатын компьютерлер беру нәтижесінде барлық ақпаратты бастапқы түрде қалпына келтіру үшін бір хаттама бойынша жұмыс істеуі тиіс. Желілік хаттамалар ақпаратты берудің әртүрлі аспектілерін басқарады, олар: физикалық байланыс, түрлі ресурстарға қол жеткізу, берілетін хабарламаны пакеттерге бөлу, деректерді беру үшін маршрутты таңдау, қателерді анықтау және т. б. Ұқсас хаттамалар топтары OSI моделінің деңгейіне сәйкес келетін аттарға ие, онда: желілік, көліктік және т. б. жұмыс істейді.

OSI нормативтері желінің келесі жұмыс істеу сәттерін сипаттайды:

- желілік құрылғылардың, оның ішінде әртүрлі хаттамаларды пайдаланатын құрылғылардың өзара әрекет етуі;
- желілік құрылғылардың әрекет ету принциптері және физикалық қосылу тәсілдері;
- деректерді берудің дұрыстығын қамтамасыз ету әдістері;
- желілік құрылғыларда үздіксіз деректер ағынын қолдау тәсілдері;
- желілік орта бойынша беру кезінде электр сигналдары түрінде деректерді ұсыну тәсілдері.

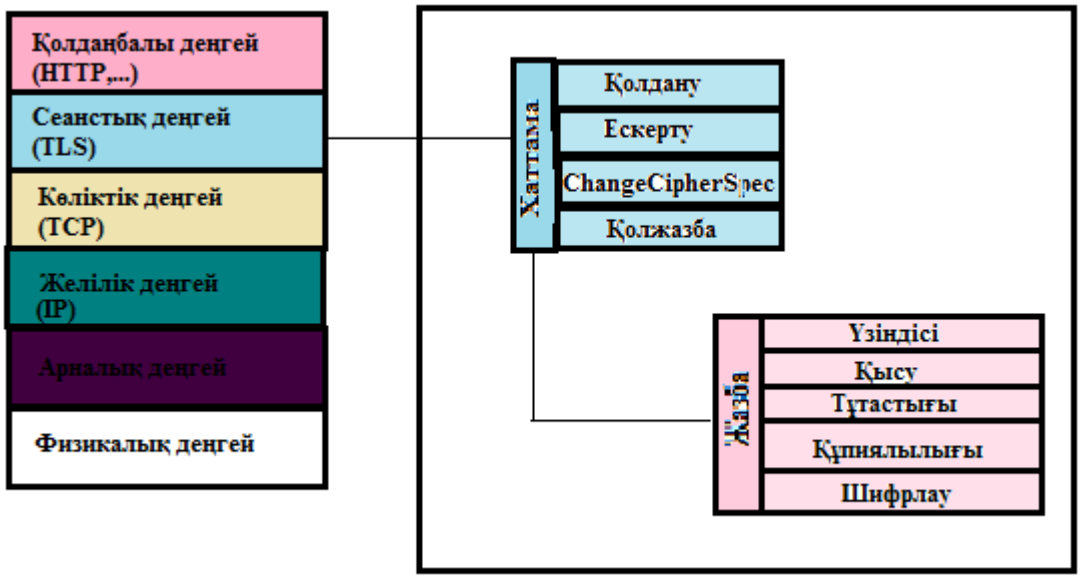
Көп деңгейлі құрылым көптеген әртүрлі өндірушілер шығарған хаттамаларды оңайлату және реттеу үшін, бағдарламалық қамтамасыз ету модульдерінен желілік жүйелерді құру үшін қолданылады. Төмен тұрған деңгейдің мақсаты-жоғары тұрған деңгейге қызмет көрсету. Әрбір деңгей тек оның жанында тұрған деңгейлермен (одан жоғары және төмен) өзара іс-қимыл жасайды. Модельдің жоғарғы деңгейі қазіргі уақытта жұмыс істейтін қосымшаға, ал төменгі – байланыс арнасы бойынша сигналдарды тікелей жіберуге сәйкес келеді.

Модельдегі ақпарат ағыны әр деңгей басқа түйіннің аттас деңгейімен тікелей өзара іс-қимыл жасайды деп болжайды. Желі тораптарының өзара

әрекеттесуін ұйымдастыру үшін жеткілікті иерархиялық ұйымдастырылған хаттамалар жиынтығы коммуникациялық хаттамалар стегі деп аталады.

Коммуникациялық хаттамалар бағдарламалық және аппараттық түрде іске асырылуы мүмкін. Төменгі деңгейдегі хаттамалар көбінесе бағдарламалық және аппараттық құралдар комбинациясымен, ал жоғарғы деңгейдегі хаттамалар – әдетте таза бағдарламалық құралдармен іске асырылады.

Модельге сәйкес, өзара іс-қимыл құралдары жеті деңгейге бөлінеді: қолданбалы, өкілді, сеанстық, көліктік, желілік, арналық және физикалық. Әрбір деңгей желілік құрылғылардың өзара іс-қимылының бір белгілі бір аспектісіне ие. OSI моделі компоненттерінің өзара әрекеттесуін келесі мысалда көрсетуге болады. Қолданба файл қызметі сияқты қолданбалы деңгейге сұрау салсын. Бұл сұраудың негізінде қолданбалы деңгейдегі бағдарламалық қамтамасыз ету стандартты форматтағы хабарды қалыптастырады. Әдеттегі хабар тақырып пен деректер өрісінен тұрады. Тақырып желі арқылы адресаттың қолданбалы деңгейіне жіберу қажет қызметтік ақпаратты қамтиды, оған қандай жұмысты орындау керектігін хабарлау үшін. Қарастырылып отырған жағдайда тақырып файлдың орналасқан жері туралы және оған қажетті операцияның түрі туралы қызметтік ақпаратты қамтуы тиіс. Хабарламаның деректер өрісі бос болуы немесе қашықтағы файлға жазылатын деректерден тұруы мүмкін. OSI моделінің сызбазы 1.1 суретте көрсетілген.



Сурет 1.1 – OSI моделіндегі SSL/TLS протоколының орны

Қолданбалы деңгейдегі желілік қосымшалардың көпшілігі HTTP, FTP және SMTP сияқты өз ақпарат алмасу хаттамаларына ие. Қолданбалы деңгейдегі хаттамалардан алынған деректерді шифрлау үшін SSL және TLS криптографиялық хаттамалары қолданылады, олар келіп түсетін пакеттерді

инкапсуляциялайды және оларды көлік деңгейіндегі хаттамамен береді. Бұл хаттамалар ашық кілтпен ассиметриялық алгоритмді шифрлау үшін пайдаланылады. SSL хабар алмасу кілттерін құру үшін RSA, Fortezza алгоритмін немесе Диффи-Хелман алгоритмінің бір нұсқасын пайдалана алады. TLS хаттамасы SSL-дың одан әрі дамуын білдіреді. TLS-да Fortezza алгоритмінің қолдауы жоқ, SSL-дан жаңа айырмашылығы криптографиялық құпиялылықты генерациялаудың күрделі механизмін қолданады.

Қолданбалы деңгей хаттамаларын толығырақ қарастырайық:

HTTPS (Hypertext Transport Protocol Secure) – бұл сайт пен пайдаланушы құрылғысы арасында деректер алмасудың құпиялылығын қамтамасыз ететін хаттама. Ақпараттың қауіпсіздігі қорғаудың 3 деңгейі бар SSL/TLS криптографиялық хаттамаларын пайдалану есебінен қамтамасыз етіледі:

1) деректерді шифрлау. Оларды ұстап алудан құтылуға мүмкіндік береді.

2) деректердің сақталуы. Деректерді кез келген өзгерту тіркеледі.

3) аутентификация. Пайдаланушыны қайта бағыттаудан қорғайды.

Қорғалған деректерді беру хаттамасын міндетті түрде пайдалану интернетте төлемдер жүргізуге қатысты барлық ақпаратты талап етеді: кез келген тәсілмен (жеке төлем картасы, онлайн төлемдер жүйесі және т.б.) интернет-дүкендерде тауарларды төлеу, интернет-банкинг арқылы қызметтерді төлеу, онлайн сервистерде (казино, online-курстар және т.б.) төлемдерді жүргізу және т.б.

HTTPS протоколының жұмысы пайдаланушының компьютері мен сервердің ортақ құпия кілтті таңдайтынына негізделген. Бұл кілт бірегей және әрбір сеанс үшін жасалады. Оны жасау мүмкін емес деп саналады, өйткені онда 100-ден астам таңба бар. Деректерді үшінші тұлғаларға ұстап алмау үшін сандық сертификат пайдаланылады – бұл серверді анықтайтын электрондық құжат. Сайттың (сервердің) әрбір иесі пайдаланушымен қорғалған байланыс орнату үшін осындай сертификат болуы тиіс.

Бұл электрондық құжатта иесінің деректері мен қолы көрсетіледі. Сертификат көмегімен сіз растайсыз:

- ол берілген адам шын мәнінде бар;
- ол сертификатта көрсетілген сервердің (сайттың) иесі болып табылады.

HTTPS протоколы бойынша қосылуды орнату кезінде браузердің бірінші жасайтын нәрсесі, бұл сертификаттың түпнұсқалығын тексеру және тек сәтті жауап берген жағдайда ғана деректерді алмасу басталады.

FTP протоколы – (File Transfer Protocol) **-** түрлі компьютерлер арасында файлдарды жылжытудың танымал және салыстырмалы қауіпсіз тәсілі. FTP деректерін беру үшін көлік хаттамасы ретінде TCP хаттамасын қолданады. Оның көмегімен пайдаланушы серверге "жеке куәлікті" көрсете алады, содан кейін қапшықтарды қарап, файлдарды екі бағытта да жібере алады. FTP деректерді клиент пен FTP сервері арасында да, екі қашықтағы компьютерлер арасында да жіберуге мүмкіндік береді.

Ол файлдарға қол жеткізу емес, ақпаратты беруді қамтамасыз етеді. FTP бойынша беру бастапқыда қауіпсіз болып табылмайды, бірақ SSL-протоколының шифрланған арнасында жұмыс істейтін FTPS хаттамасы деректерді қауіпсіз беруді қамтамасыз етеді. Бұл пәрмендерді және берілетін деректерді қорғауға мүмкіндік береді.

FTPS серверлері ашық кілт сертификаттарын ұсынады. Әдетте, олар Unix құралдарын немесе OpenSSL сияқты Windows үшін бейімделген құралдарды пайдалану арқылы жасалады. Әрбір сертификатқа сертификаттау орталығы қол қоюы тиіс. Басқа жағдайда FTPS клиенті ескерту жасайды. Деректерді арналық деңгейде кодтауға болады (командалар және/немесе деректер). FTPS протоколы екі байланысты пайдаланады: біреуі деректерді береді; екіншісі-серверге командалар және оларға сервердің жауаптарын береді. Егер SSL базасында шифрлау қолданылса, деректер алмасу үшін порт нөмірі туралы мәліметтер қолжетімсіз болады.

SMTP (ағылш. Simple Mail Transfer Protocol) - бұл TCP/IP желілерінде электрондық поштаны жіберуге арналған кең қолданылатын желілік хаттама.

SMTP стандартында пошта хабарламаларын жіберу кезінде шифрлау да, аутентификация процедурасы да пайдаланылмайтындықтан, кез келген хабар көру үшін қол жетімді болып табылады. Барлық шешімдер клиент жағында, мысалы, Secure MIME (S/MIME) немесе Pretty Good Privacy (PGP) сияқты заттар, поштаны қорғау мәселесін шешуге көмектесе алады, бірақ олар осы рәсімге пайдаланушылардың қатысуын талап етеді. Қауіпсіздік үшін күш-жігерді шоғырландыру қажет негізгі учаске-SMTP трафигін қорғау. Егер SMTP қауіпсіздігі қамтамасыз етілсе, онда негізінен пошта трафигінің жүз пайыз қауіпсіздігіне қол жеткізуге болады.

Microsoft Exchange Server пошта трафигінің қауіпсіздігін қамтамасыз етудің бірнеше тәсілдерін көздейді. Олардың бірі бар қосылыстар үшін Secure Sockets Layer (SSL) for SMTP міндетті түрде қолданудан тұрады. Алайда, бұл әдісті қолдану кейбір мәселелерді тудырады. Әдепкі бойынша барлық SMTP серверлері 25 портты пайдаланады. Бірақ, егер 25-ші портқа SSL қолданылса, онда SSL қолдамайтын қалған серверлер 25-ші порт арқылы осы сервермен байланысты орната алмайды. Ал егер порттың стандартты емес нөмірін пайдалансаңыз, қалған серверлер оны анықтай алмайды.

Мәселені айналып өтуге болады. STARTTLS командасы (ол Extended SMTP — ESMTP құрамына кіреді) клиент пен SMTP серверіне қарапайым SMTP-қосылу үшін Transport Later Security (TLS) қолдану фактісін тануға мүмкіндік береді. Қосылу қатысушысы оның кез келген соңында өзінің әріптесін немесе TLS-қосылымды тек құпия байланыс арнасы ретінде пайдалана алады. Қалай болса да, мұндай тәсілде үш маңызды артықшылығы бар:

- қалған серверлермен және клиенттермен қиылысу жоқ. STARTTLS функциясын қолдайтын клиенттер оны пайдалана алады; қарсы жағдайда, SMTP қорғалмаған трафигімен жұмыс істеуді жалғастырады;

- шешім икемділігі. Егер клиент TLS SMTP-мен іске қосса, сервер басқа серверлерге жүгінген кезде TLS-қосылымдарын автоматты түрде сұратады және TLS-қосылым туралы сұрауларға өзі жауап береді. Мысалы, кез келген сыртқы сервер абоненттерді келісу процесін іске қосты, бұл жағдайда пошта автоматты түрде қорғалған болады. Дегенмен, мен әкімшілерге пайдаланушыларға пошта клиентінде SSL/TLS параметрін қосуға кеңес берер едім;

-SMTP шифрлауы хабарламалардың тақырыптарын қорғайды, бұл трафиктің анализатор-бағдарламаларынан қорғаудың қосымша дәрежесі, онсыз қаскүнем бір-бірімен кім және қалай жиі байланысатынын оңай анықтай алатын еді.

Бір маңызды ескерту: TLS бүкіл байланыс бойына, яғни, байланыс орнатылған кезден соңына дейін хабарламаны қорғамайды. Басқаша айтқанда, хабарлама клиент станциясында сақталған жағдайда немесе клиенттен серверге жіберілген кезде (Егер клиент өзі TLS қолдамаса) қорғалмаған. TLS хабарламаны TLS қолдайтын екі сервердің арасында жіберілгенге дейін қорғайды.

1.1 Ақпараттық қауіпсіздік үшін хаттаманың маңыздылығы

Transport Layer Security (TLS) хаттамасы – Secure Sockets Layer (SSL) қабылдағышы, әлемдегі ең танымал криптография қосымшасы болып табылады. Әдетте хаттама веб-браузермен жұмыс істеу сеанстарын қорғау үшін қолданылады, бірақ ол басқа тапсырмаларды шешу үшін кеңінен қолданылады, мысалы, электрондық пошта серверлерін қорғау, клиент-серверлік транзакцияларды қорғау және т.б. TLS сияқты VPN туннелдеуді қамтамасыз ету, сеанс орнату протоколын (Session Initiation Protocol (SIP) аутентификациялау және шифрлеу үшін де қолданылуы мүмкін. SSL / TLS байланыс сеансының екі жағын сенімді аутентификациялау, деректерді шифрлау және жіберу кезінде олардың бүтіндігін тексеру функцияларын ұсынады. Соңғы бірнеше жылда протоколдың архитектурасы мен жүзеге асырылуының кемшіліктерін, сондай-ақ пайдаланылатын криптографиялық алгоритмдердің осалдығын пайдаланатын түрлі шабуылдар жасалды.

TLS хаттамасының негізгі мақсаты екі бағытта да еркін деректерді беру үшін пайдаланылатын байланыс арнасын тыңдаудан қорғалған желінің екі торабы арасында құру, олардың бүтіндігін тексеру, сондай-ақ тараптардың аутентификациясын қамтамасыз ету болып табылады.

TLS қатерлерінің моделі шабуылдаушының байланыс арнасына толық қол жетімділігі бар деп болжамдайды, мысалы, пакеттерді белсенді ауыстыруы, каналдағы байланысты үзуі мүмкін. Сондықтан TLS протоколының негізгі міндеттері:

- берілетін деректердің құпиялылығын қамтамасыз ету;
- берілетін ақпараттың тұтастығын тексеруді іске асыру;
- екі жақты аутентификацияны қамтамасыз ету.

TLS хаттамада көрсетілген міндеттерді орындау үшін тараптарды аутентификациялау және сеанстық кілтті, генерациялау үшін асимметриялы криптографияны, байланыс сеансы ішінде деректердің құпиялылығын сақтау үшін симметриялы криптографияны, хабарламалардың тұтастығын бақылау үшін хабарламаларды аутентификациялау кодтарын пайдаланады.

Байланыс орнату процедурасының хабарламаларынан басқа, шифрлау барлық хабарламалар үшін пайдаланылады, сонымен қатар, тараптардың аутентификациясы опциональды жүзеге асырылады.

1.2 SSL/TLS хаттамасының компоненттері.

TLS хаттамасында шифрлау алгоритмдерін таңдау қосылысты орнату барысында жүзеге асырылады және сервер мен клиенттің мүмкіндіктеріне байланысты.

TLS хаттамасы бойынша аутентификация процесі екі кезеңнен тұрады:

- сервердің түпнұсқалығын анықтау;
- түпнұсқалығын міндетті түрде анықтау.

Бірінші міндетті кезең:

1) сервер клиенттің сұрауына жауап ретінде өзінің сертификатын және шифрлау параметрлерін жібереді.

2) клиент мастер-кілтті жасайды, оны сервердің ашық кілтімен шифрлайды және серверге жібереді.

3) сервер мастер-кілтті өзінің құпия кілтімен ашып, клиенттің мастер-кілтімен расталған хабарламаны қайтара отырып, өзінің түпнұсқалығын растайды.

4) келесі деректер шифрланады және осы кілттің негізінде алынған кілттермен расталады.

Шебер-кілтті білмей, ағымдағы уақытта деректер шифрланатын ағымдағы кілтті анықтау мүмкін емес.

Міндетті болып табылмайтын екінші кезеңде сервер клиентке сұраныс жібереді, ал клиент серверге өзінің цифрлық қолтаңбасы бар сұрау салуды және ашық кілт сертификатын қайтара отырып, өзінің түпнұсқалығын растайды.

SSL/TLS қауіпсіз протоколы екі протоколдың арасында орналастырылады: бағдарлама-клиент (HTTP, FTP, IMAP, LDAP, Telnet және т.б.) және TCP/IP транспорттық протоколы.

Екі жағынан да, өз түрін жасай отырып, ол деректерді қорғайды және көлік деңгейіне береді. Көп қабатты принцип бойынша SSL/TLS протоколы көптеген әр түрлі клиент-бағдарламалардың хаттамаларын қолдай алады.

Хаттама жұмысын екі деңгейге бөлуге болады:

1)қосылысты растау хаттамасының қабаты (Handshake Protocol Layer)

2)жазба протоколының қабаты

Бірінші қабат, өз кезегінде, үш подротоколдан тұрады:

1) қол алысу хаттамасы - Handshake Protocol;

2) шифрлау параметрлерін өзгерту хаттамасы - Cipher Spec Protocol;

3) ескерту хаттамасы-Alert Protocol.

Қол алысу хаттамасы клиент пен сервер арасында сессия деректерін келісу үшін пайдаланылады. Осы сессияға:

- сессияның сәйкестендіру нөмірі;
- екі тараптың сертификаттары;
- шифрлау алгоритмінің параметрлері;
- ақпаратты қысу алгоритмі.

Қол алысу хаттамасы деректермен алмасу тізбегін жүргізеді,бұл өз кезегінде тараптардың аутентификациясын бастайды және шифрлауды, хэширлеуді және қысуды келіседі. Келесі кезең-қосылымды растау хаттамасымен жүзеге асырылатын қатысушыларды аутентификациялау.

Шифрлау параметрлерін өзгерту хаттамасы шифрлау кілттерін жасау үшін қолданылатын кілт деректерін (keyingmaterial) өзгерту үшін қолданылады. Хаттама сервер жіберуші кілттер жинағын өзгертуді қалайтын бір хабардан тұрады.

Ескерту хаттамасында тараптарға мәртебесінің өзгеруін көрсететін немесе ықтимал қате туралы хабарлайтын хабарлама болады. Әдетте, байланыс жабылған және қате хабар алынған кезде ескерту жіберіледі, хабарды шифрлеу мүмкін емес немесе пайдаланушы әрекетті жояды.

Жазба хаттамасы бірнеше деңгейден тұрады. Қолданбалы деңгейден түсетін хабарламалар ұзындығы 16 Кбайтқа дейінгі блоктарға фрагменттеледі. Егер қысу көзделсе (рәсім міндетті емес), әрбір блок тәуелсіз қысылады.

Содан кейін әрбір деректер блогына хабарларды аутентификациялау коды қосылады. SSL/TLS-да хабарларды аутентификациялау үшін стандартты HMAC-хабарды аутентификациялау коды қолданылады.

Келесі қадам-MAC мәнімен бірге деректер блогын шифрлау. Шифрлау симметриялы кілтпен криптография көмегімен жүргізіледі.

SSL/TLS жұмысының соңғы қадамы-тақырыпты қосу:

- деректер блоктары TCP – қосылу арқылы берілетін қолданбалы деңгей протоколының сәйкестендіргіші;
- сығылған фрагменттің ұзындығы.

Қосылыстың басқа соңында алынған деректер шифрленеді, олардың бүтіндігі тексеріледі, одан әрі олар декомпрессацияланады, дефрагментацияланады және неғұрлым жоғары деңгейдегі хаттамаларға беріледі.

1.3 Қол алысу хаттамасының жұмыс алгоритмі

SSL/TLS протоколдары үш аутентификация режимін қолдайды:

1) тараптардың өзара аутентификациясы;

2) серверді бір жақты аутентификациялау (клиентті аутентификациялаусыз);

3) толық анонимдік.

Соңғы нұсқада өзара іс-қимыл жасайтын тараптар қатысушылардың ауысуымен байланысты ықтимал шабуылдардан қорғалмайды, бірақ бұл ретте орнатылған қосылыстың санкцияланбаған кіруінен қорғау қамтамасыз етіледі.

TLS хаттамасына сәйкес клиент пен сервер арасында қорғалған өзара іс-қимыл режимін орнату рәсімі мынадай түрде көрінеді (клиент тарапынан серверді бір жақты аутентификациялау нұсқасы қарастырылады):

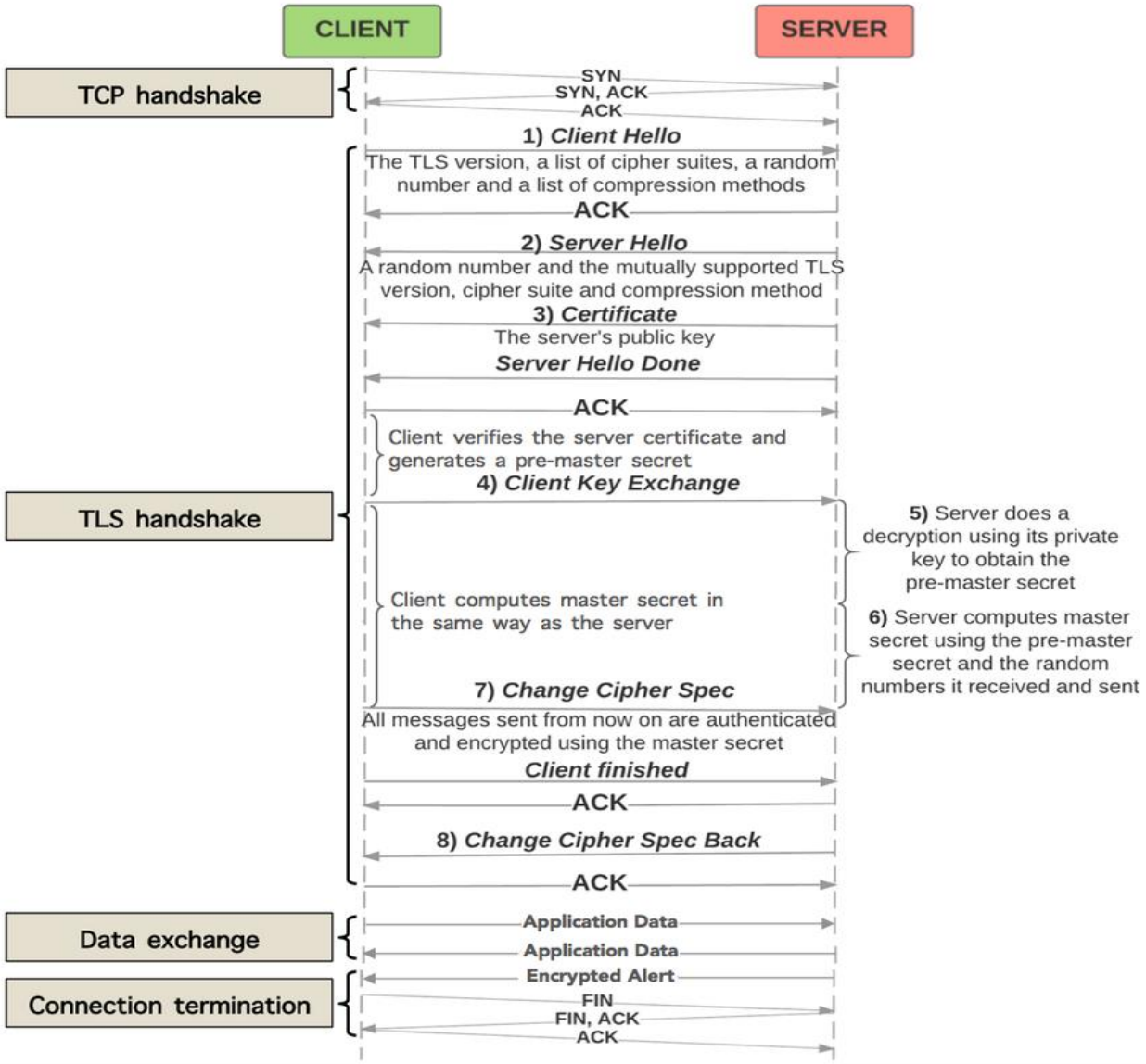
- клиент пен сервер сеанстарда қолданылатын алгоритмдер мен қорғау параметрлері туралы келіседі, кездейсоқ мәндердің client_random - 32 байты, server_random шамаларымен алмасады. сондай-ақ, жаңа қосылыстар болатынын немесе болмайтынын анықтайды;

- клиент пен сервер клиент пен серверді аутентификациялау үшін сертификаттармен алмасады;

- клиент pre_master secret кездейсоқ шамасын жасайды, оны шифрлайды және серверге береді;

- клиент және сервер pre_master secret, client_random және secret_random master secret сеансты қалыптастырады.

"Қол алысу "SSL / TLS –сессиясын орнату кезеңі толық түрде төменде көрсетілген (1.2-сурет):



Сурет 1.2 - Қол алысу кезеңі

SSL/TLS-қосылуды орнату хаттамасында бірінші хабар Client Hello хабарламасы болып табылады. Хабарлама келесі деректерді қамтиды:

1) хаттама нұсқасы- клиент қолдайтын ең жоғарғы нұсқа;

2) 32 байт кездейсоқ мәндер-client_random. Бастапқыда, спецификацияда UNIX-таймстампаларды беру үшін алғашқы 4 байтты пайдалану, ал қалған 28 - і жалған кездейсоқ сандардың криптографиялық генераторының жұмыс нәтижесін толтыру ұсынылды. Дегенмен, қазір көптеген браузерлер мен веб-серверлер барлық 32 байтты кездейсоқ жасайды. Сәл алға жүгіре отырып: handshake - хабарламаларда таймстамптың болуы сол немесе басқа торапта уақыт ауыстырумен байланысты проблемаларды табу кезінде көмектесе алады деп болжалды. Алайда, бұл әдіс қазір қолданылмайды,сондықтан барлық client_random байттары кездейсоқ. Мұндай тәсіл TLS 1.3-да бекітілген;

3) TLS-сессиясының идентификаторы-SessionID: TLS қосылымды орнату хаттамасының қысқартылған нұсқасын пайдалана отырып, бұрын орнатылған сессияларды қайта жаңартуға мүмкіндік береді. Сессия

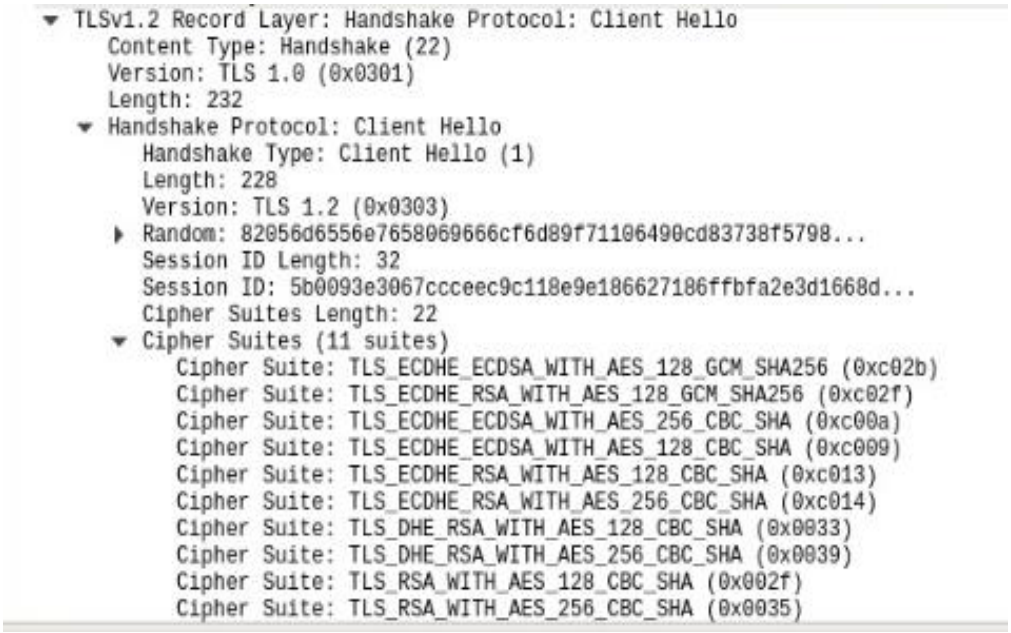
идентификаторы параметрлері серверде сақталған сессия нөмірін қамтиды (осы опцияны төменде қарастырайық). TLS 1.3-де бұл өріс бос болуы мүмкін, ал егер бар болса, онда басқа рөл атқарады: Client Hello - да Session ID өрісін табу арқылы сервер оның мәнін өзгертусіз өз жауабына қосады, сонымен қатар 1.3-де sessionid-сессия нөмірі ретінде пайдаланылмайды, бірақ 1.2-нұсқа сессияларын имитациялау құралы бола алады.;

4) Cipher Suites клиент қолдайтын шифрлау тізімі. Тізімдегі шифрлау тізімінің тәртібі клиентпен олардың артықшылық дәрежесін көрсетеді (таңдаулылары бірінші болып беріледі), бұл тәртіп - тек ұсыныс және сервер әрқашан оған жүгінбейді;

5) қолдау көрсетілетін сығу әдістерінің тізімі-compression methods, тәртіп бұл кезде тағы да таңдау дәрежесіне сәйкес келеді, бірақ әдетте бұл өрісте тек бір ғана мән - null, өйткені сығуды пайдалану ұсынылмайды. TLS 1.3 - де-қысуға тікелей тыйым салынады, бірақ "тарихи себептер" бойынша, бұл өріс null тіркелген мәнімен сақталады;

6) Хаттаманың бірнеше кеңейтулерінің деректері.

Client Hello хабарламасын төменнен көруге болады (сурет 1.3):



Сурет 1.3- Wireshak-тағы қол алмасу кезеңі (Client Hello)

Client Hello хабарламасындағы әрбір өрістің өз пішімі бар, ал өріс ұзындығы туралы деректер кеңейтілгенде қосымша тақырып алдында болады. Тақырып әдетте кеңейтім түрі мен оның деректерінің ұзындығын қамтиды. Мұндай құрылым іске асыру кезінде хабарларды дұрыс бөлуге мүмкіндік береді.

Егер сервер Client Hello өңдесе, онда ол Server Hello хабарламасына жауап береді. Бұл хабар төрт байттан тұрады: хабар түрі (бір байт) және ұзындығы (үш байт). Server Hello (мұнда 1.3-ге дейінгі нұсқаларды қарастырамыз) келесі өрістерді қамтиды:

1) клиент пен сервер пайдаланатын хаттама нұсқасы;

2) 32 байтты кездейсоқ мәндер-server_random. Бұл кезде де жағдай client_random сияқты: алғашқы төрт байт таймстамп болуы мүмкін жәнеболмауыда мүмкін. Егер сервер уақыттың дұрыс мәніне жауап берсе, онда Handshake хабарламаларының толық жиынтығында деректердің бүтіндігін криптографиялық куәландыратын хабарлама бар екенін ескере отырып, сервермен қол қойылған оның сағаты бойынша қосылу уақыты туралы түбіртекті аламыз, секундқа дейін дәлдікпен аламыз-кейде бұл деректер сервер әкімшілігінің мекенжайына сервердің логынан жазбаларды алу туралы сұрау салуды дұрыс жасауға көмектеседі;

3) жаңа сессияға сервер берген session id – сессия идентификаторы (tls 1.3 жағдайында - бұл өріс клиенттің Session ID-ін міндетті түрде қайталайды);

4) Cipher Suite шифрлау серверімен таңдалған және бұл шифронаборды клиент пен сервер одан әрі қолданады. Сервер клиент ұсынған ClientHello-да шифронаборды таңдайды, бірақ клиенттің басымдылығы міндетті емес: сервер тек қалаған шифронаборды өзі анықтайтын кері жағдай ғана таралған;

5) сервермен таңдалған қысу әдісі-бұл null;

6) кейбір кеңейтімдер жиынтығы.

Server Hello хабарламасын төменнен көруге болады (сурет 1.4):

Сурет 1.4 – Wireshak-тағы қол алмасу кезеңі (Server Hello)

Клиент алынған сервер сертификатын өзіне белгілі ЦС ашық кілтінің көмегімен тексереді.

Тексеру нәтижесі оң болған жағдайда клиент келесі әрекеттерді орындайды (тексеру нәтижесі теріс болған жағдайда сессия жабылады):

1) Pre_MasterSecret (тек сервер мен клиентке белгілі ортақ құпия бөлігі) кездейсоқ 48 - байталы тізбегін жасайды; сервер сертификатында алынған сервердің ашық кілтінде шифрлайды және серверді жібереді;

2) келісілген хэш-алгоритмдердің көмегімен басты бірлескен құпия (mastersecret) қалыптастырады, параметрлер ретінде алдыңғы қадамда серверге жіберілген Pre_mastersecret бірлескен құпиясының бір бөлігін және одан алынған Server_random кездейсоқ тізбегін пайдаланады;

3) MasterSecret қолдана отырып, сеанстың криптографиялық параметрлерін есептейді: сервермен ортақ сеанстық құпия кілттерді симметриялық шифрлау алгоритмі (қабылдау және беру үшін) және MAC есептеу құпияларын қалыптастырады;

4) қорғалған өзара әрекеттесу режиміне өтеді.

Сервер клиент тапсырған сертификатты тексереді.

Сервер алынған Pre_MasterSecret құпия кілтінің көмегімен шифрлейді және клиент сияқты операцияларды орындайды:

1) келісілген хэш-алгоритмдердің көмегімен басты бірлескен құпия (MasterSecret) қалыптастырады, алдыңғы қадамда клиентке жіберілген PreMasterSecret параметрлері ретінде Secret_random кездейсоқ тізбегі және одан алынған Client_random кездейсоқ тізбегі қолданылады;

2) MasterSecret-ті қолдана отырып, сеанстың криптографиялық параметрлерін есептейді: клиентпен ортақ сеанстық құпия кілттерді шифрлау алгоритмі және MAC есептеу үшін құпия қалыптастырады;

3) қорғалған өзара әрекеттесу режиміне өтеді.

SSL / TLS – сессиясының параметрлерін қалыптастырған кезде клиент пен сервер бірдей бастапқы деректерді (келісілген Алгоритмдер, Pre_MasterSecret жалпы құпия және Client_random және Server_random кездейсоқ тізбектерімен) пайдаланғандықтан, жоғарыда сипатталған әрекеттердің нәтижесінде олар жіберілетін хабарламалардың бүтіндігін қорғау үшін қолданылатын шифрлаудың бірдей сеанстық құпия кілттерін және құпияларды әзірледі. SSL / TLS-сессия параметрлерімен бірдейлікті тексеру үшін клиент пен сервер бір-біріне мазмұны Тараптардың әрқайсысына белгілі мәтіндік хабарламаларды жібереді.

TLS заманауи іске асыруларында "кеңейтулер" (Extensions) бөлімі өте үлкен мәнге ие, өйткені онда клиент пен сервердің жұмыс сызбасын анықтайтын параметрлер беріледі. Сервердің мақсаты - байланыс параметрлерін келістіру. TLS жақсы белгілі "сұрау-жауап-растау" схемасын пайдаланады (қосылысты жедел орнату нұсқасынан басқа), ал Client Hello және Server Hello хабарламалары схеманы іске қосады. Бұл хабарламаларда ешқандай құпия ақпарат жоқ , тиісінше-ашық түрде беріледі (TLS 1.3 жағдай өзгерді-Handshake хабарлары шифрланған түрде дереу жіберіледі, дегенмен, Server Hello және бірқатар кеңейтулер әлі де ашық). Бұл хабарлар, әсіресе-Client Hello, барлық жерде DPI жүйелерінде TLS-қосылыстарды анықтау (немесе анықтау әрекеті) фактісін анықтау үшін қолданылады.

1.4 SSL және TLS нұсқаларын салыстыру

Желінің тораптары арасында қорғалған деректерді беруді қамтамасыз ету тиімділігі едәуір дәрежеде қолданылатын криптографиялық хаттамаға байланысты. Қазіргі уақытта TLS 1.1 және TLS 1.2 хаттамаларын пайдалану орынды болып табылады, өйткені хаттамалардың осы нұсқаларында белгілі осалдықтар жоқ, алайда Интернет желісіндегі коммуникациялардың бір бөлігі бұрынғысынша ерте нұсқалардың хаттамаларымен шифрланады,бұл берілетін

ақпараттың құпиялылығына қауіп төндіреді. TLS 1.1-ден бұрын ұсынылған криптографиялық хаттамаларды пайдалану ақпараттың сақталуына кепілдік бермейді, өйткені SSL 2.0, SSL 3.0 және TLS 1.0 хаттамаларында болуы ақпараттық шабуыл болған жағдайда зардаптарды болдырмауға мүмкіндік бермейтін сыни осалдықтар бар.

Төменде өзгертілген параметрлер жаңа нұсқамен қосылған:

1) SSLv3.0:

- хабар таратудан деректерді бөлу;
- клиент пен сервердің сертификаттар тізбегін жіберу мүмкіндігі, бұл ұйымдарға екі сертификаттан тұратын сертификаттар иерархиясын пайдалануға мүмкіндік береді;
- RSA пайдаланбайтын сертификаттармен қатар Диффи-Хеллман және Fortezza алгоритмі бойынша кілттермен алмасуды ұйымдастыруға мүмкіндік беретін кілттермен алмасу хаттамасын іске асыру;
- жазбаны қысу және ашу мүмкіндігі.

2) TLSv1.0:

- кілтті алудың түрлі функциялары;
- модификациялық MAC – HMAC құралын пайдалану;
- көбірек хабарламалар;
- DSS/DH қолдау қажет.

3) TLSv1.1:

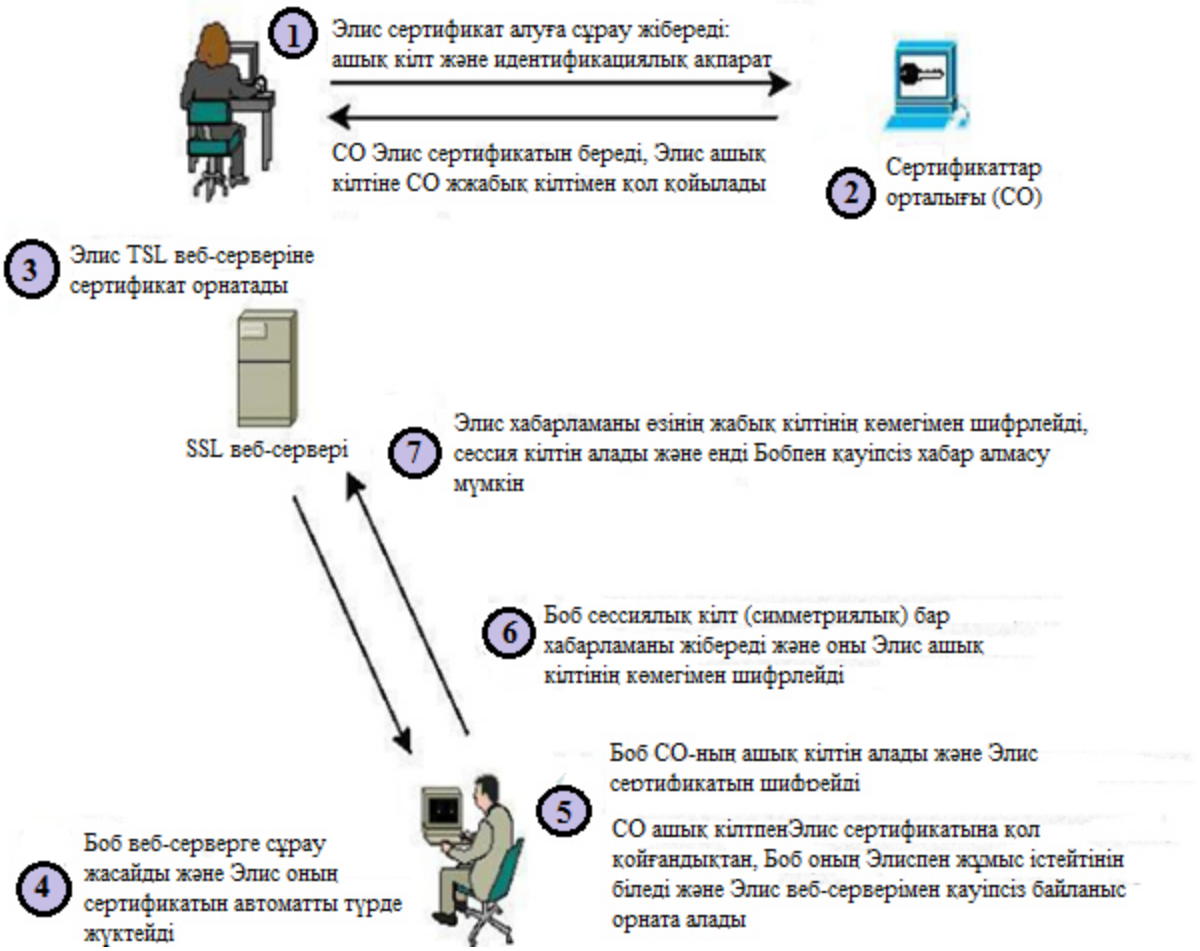
- инициализацияның айқын емес векторы CBC шабуылдарынан қорғау үшін айқынға ауыстырылды;
- қателерді өңдеу басқа ескертулерді пайдалану үшін ауыстырылды.

4) TLSv1.2:

- Md5 / sha1 жалған кездейсоқ функциядағы комбинациясы cipher-suite-specified псевдорандом функциясымен ауыстырылады;
- сандық қолтаңба элементтеріндегі md5/sha1 комбинациясы бір хешемен ауыстырылады. Қол қойылған элементтер хешті қолданатын алгоритмді анық көрсететін өрісті қамтиды;
- деректер үлгілерін қосу арқылы аутентификация шифрлау қолдауы қосылды;
- TLS кеңейтімдері және AES шифрларының жиынтығы біріктірілген;
- EncryptedPreMasterSecret нұсқаларының нөмірлерін қатаң тексеру.

1.5 Хаттама жұмысының мысалы

Хаттама жұмысын көрсету үшін БОБ пайдаланушысы мен ЭЛИС веб-сервері арасында хабар алмасу көрсетілген (1.5-сурет). Веб-серверге кіру үшін БОБ пайдаланушы браузерді пайдаланады.



Сурет 1.5 – Хаттама жұмысының мысалы

Веб-сервер өз жұмысын бастамас бұрын, ол сертификаттау орталығы (СО) қол қоятын сертификатты алуға және орнатуға тиіс.

Элис сертификат алу үшін:

- сертификат алу сұрауын жасау:
- екі ашық және жабық кілттерді құрастыру;
- элис компаниясы туралы ақпарат және ашық кілт бар сертификат алу үшін сұрау жасау;
- сертификаттау орталығына сұрау жіберу.

1) оң нәтиже болған жағдайда сертификациялық орталық сертификат орталығы қол қойған элис ашық кілт және сертификат бар Элис жауабын жібереді;

2) одан әрі Элис сертификатты веб-серверде сертификаттар базасына орналастырады;

3) Боб Элис веб-серверіне сұрау жібереді, қол алысу кезінде автоматты түрде сертификатты жүктейді;

4) Боб браузері сертификатты тексереді, енді Бобта ашық Элис кілті бар;

5) Боб Элис ашық кілтінің көмегімен шифрланған сеанстық кілт бар Элис хабарын Элиске жібереді;

6) Веб-сервер сеанстық кілт бар Бобтан хабар алғаннан кейін, ол оны өзінің жабық кілтімен шифрлейді.

2 TLS протоколының белгілі осалдықтары мен шабуылдарын зерттеу

Соңғы бірнеше жылда TLS протоколының қауіпсіздігін, олар қолданатын криптографиялық алгоритмдерді, оны жүзеге асыруды көптеген зерттеулер жүргізілді. Нәтижесінде хаттаманың бірнеше маңызды осалдықтары табылды,олардың кейбіреулері үшін сәтті шабуылдар ұсынылды. Нәтижесінде хаттаманың белгілі осалдықтарын және олармен байланысты т.б. зерттеу қажеттілігі туындайды. Зерттеу қорытындысы бойынша неғұрлым маңызды осалдықтар тізбесін бөліп көрсету, олардың клиенттер мен серверлердің конфигурацияларында болуын тексеру әдістемесін әзірлеу, соңында қорғау бойынша ұсыныстар қалыптастыру қажет.

2.1 Heartbleed (CVE-2014-0160)

Heartbleed- серверде немесе клиентте, оның ішінде сервердің жабық кілтін алу үшін жадты рұқсатсыз оқуға мүмкіндік беретін OpenSSL криптографиялық бағдарламалық қамтамасыз етуінде буфердің толып кету осалдығы. Осалдық 2011 жылғы 31 Желтоқсанда TLS Heartbeat кеңейтуді қолдаумен бірге енгізілді және OpenSSL 1.0.1 нұсқасымен 2012 жылғы 14 наурызда таратылды. 2014 жылғы 7 сәуірде OpenSSL 1.0.2-beta нұсқасы және 1.0.1 алдындағы барлық 1.0.1 нұсқаларының TLS Heartbeat кеңеюін іске асыруда жадымен жұмыс істеудің сыни қатесі бар деп жарияланды.

Heartbeat кеңейтімі клиент пен сервер арасында бос тұрып қалу кезіне байланысты сақтауға арналған. Ол үшін клиент периодты түрде кейбір деректер мен кездейсоқ толтырушы байттардың пакетін қалыптастырады және оларды сервер өзгермеген түрде қайтаруы тиіс (бұл сервер пакеттің шифрын шешкеніне кепілдік береді). Осалды OpenSSL бұл пакеттің дұрыстығын тексермейді, бұл бұзушыға 64 кБ (екібайт өлшемі өрісі) дейінгі деректер ұзындығы көрсетілген және деректер жоқ heartbeat-сұрауды қалыптастыруға мүмкіндік береді. OpenSSL нұсқасының қатесіне ұшыраған нұсқасы буфердің шегінен шығып, шабуылшыға арналмаған деректерді алуға мүмкіндік бере отырып, клиентке қажетті жадты бөліп береді.

Heartbleed арқылы белгілі бір жад блогын шығаруға болмайды. Алайда зиянкестер келесі талдау үшін деректердің барынша көп көлемін алу үшін шабуылдарды бірнеше рет қайталай алады. Осылайша, бұзушы сервердің құпия деректерін (жабық кілтті, cookie файлдарын, пайдаланушылардың сұраулары мен жауаптарын) ала алады.

2.2 ChangeCipherSpec (CVE-2014-0224)

CCS (CVE-2014-0224) шабуылы OpenSSL кітапханасындағы сеанс параметрлерін келісу процедурасын жүзеге асырудағы қатеге негізделеді. Қате ChangeCipherSpec хабарламасын TLS хаттамасында ұйғарылған хаттамадан өзгеше келісу процедурасы кезеңінде қабылдау мүмкіндігі болып табылады.

Қате бұзушыға байланыс арнасында ChangeCipherSpec хабарын клиент пен серверге тараптар сеанс кілтін орнатқанға дейін жіберуге мүмкіндік береді. Сәтті шабуыл сеанстың екі жағында осал болған жағдайда ғана мүмкін болады. SSL/TLS протоколының барлық нұсқалары және криптографиялық алгоритмдердің барлық жиынтығы шабуылға ұшырайды.

Осалдықтан қорғау үшін пайдаланушылар OpenSSL түзетілген нұсқаларын пайдалану қажет:

- OpenSSL 0.9.8 0.9.8 za төмен емес нұсқасы қажет;
- OpenSSL 1.0.0.0 төмен емес нұсқасы қажет;
- OpenSSL 1.0.1 1.0.1 төмен емес нұсқасы қажет.

2.3 Secure Renegotiation (CVE-2009-3555)

SSL/TLS сеанс параметрлерін қайта қарау ресімі бұзушымен байланыс арнасында жүзеге асырылатын белсенді шабуылға осал болып келеді. Тәртіп бұзушы сервермен TLS сеансын орната алады, қажетті деректерді жіберіп, содан кейін сеансты клиенттің жаңа сеансымен біріктіре алады. Сервер параметрлерді қайта қарау ретінде клиенттік келісуді өңдейді, ал бұл бұзушы берген деректер мен клиенттің кейінгі деректері заңды клиенттен алынған деректер ретінде қабылданатынын білдіреді.

Қайта қарау рәсімі бірінші келісу кезінде белгіленген криптографиялық параметрлерді пайдалана отырып орындалады, бірақ олардың арасында қандай да бір криптографиялық байланыс жоқ. Бұл трафикті ұстап қалу мүмкіндігі бар бұзушыға екі тарап үшін де клиент пен сервердің өзара іс-қимылының басында өз деректерін қосуға мүмкіндік береді.

Шабуылдарды бастау үшін бұзушы сервермен TLS сеансын орнатады, содан кейін қажетті деректерді серверге жібереді. Осыдан кейін тәртіп бұзушы клиентке сеанс параметрлерін сервермен келісу рәсімін жүргізуге мүмкіндік береді. Келісуді аяқтағаннан кейін клиент сеанс қауіпсіздігінің жаңа параметрлерін пайдалана отырып, сервермен өзара іс-қимыл жасайды. Бұзушы жіберілген хабарламаларды оқи алмайды, бірақ сервер бұзушының бастапқы хабарламасын клиент жібергенін болжайды.

HTTPS хаттамасында алдын - ала және пост-аутентификация бірдей шарттарда жүргізіледі, осылайша, сертификатпен аутентификацияны пайдаланатын клиенттер шабуылға осал. Мұндай шабуыл парольдерді ашу үшін пайдаланылуы мүмкін: бұзушы префикс ретінде клиенттің іс-әрекетін логирлеу командасын оған қол жетімді аймаққа жібереді, содан кейін клиент өз паролін серверде енгізеді, ол бұзушының логында сақталады.

Мұндай шабуылдан қорғау үшін сеанс параметрлерін қайта қарау және бастапқы келісу рәсімдері арасындағы криптографиялық байланысты қосатын TLS протоколының сигналдық кеңеюін пайдалану қажет. Серверлер осы кеңейтуді қолдамайтын клиенттер үшін параметрлерді қайта қарау рәсіміне тыйым салуға міндетті.

2.4 Secure Client-Initiated Renegotiation

SSL/TLS сеанс параметрлерін келісу және соның салдарынан қайта қарау серверден клиенттен келісу және 15 есе үлкен есептеу шығынларын талап етеді. Бұл кемшілік секундына SSL/TLS сеанстарын сұрайтын бұзушыға сервердің процессорын есептеулермен толық жүктеуге мүмкіндік береді.

Клиент бастама жасайтын сеанс параметрлерін қайта қарау процедурасы бұзушының DoS-шабуылына жұмсаған ресурстарын бір TCP қосылу үшін серверді ресурсыйымды есептеулермен жүктей отырып, одан әрі азайтады.

Серверлер әдетте дәстүрлі DoS / DDoS шабуылдарына дайындалған: арнаның өткізу қабілеті және есептеу ресурстары клиенттерден үлкен трафик көлемін өңдеуге қабілетті. Қалыпты жұмыс режимі үшін SSL/TLS сеанс параметрлерін келісу клиентпен қосылудың басында ғана жүзеге асырылады, сеанстың қалған бөлігі сервердің үлкен есептеу шығындарын талап етпейді. Сондықтан сервер сеанс параметрлерін келісу/қайта қарау процедураларының көп санын өңдеуге дайын емес.

Орташа өнімділік сервері секундына 300 келісу процедураларын өңдеуге қабілетті. Кәдімгі ноутбук процессорды 10-25% жүктеу кезінде сұраулар санын орындай алады. Осылайша, 30 гигабитті қосылымы бар сервер үшін баяу DSL қосылымын пайдаланатын ноутбук қаупі болады.

Сәтті шабуылдан болатын тәуекелді азайту клиент бастамашылық жасайтын сеанс параметрлерін қайта қарау мүмкіндігін ажыратқан кезде мүмкін болады: Microsoft IIS клиент бастамашылық жасайтын параметрлерді қайта қарауды қолдамайды, Apache қолдау көрсетті, бірақ Secure Renegotiation (CVE-2009-3555) қорғау үшін RFC 5746 іске асырылғаннан кейін өшірді. Клиент бастамашылық жасаған қайта қарауды қолдауды өшіру серверді үлкен есептеу ресурстары бар және қызмет көрсетуден бас тартудың бөлінген шабуылын жүргізуге қабілетті бұзушыдан қорғамайды. Табысты DDoS шабуылды іске асырудан болатын тәуекелді төмендету жоғары өнімді есептеулерді орындау функцияларын өзіне алатын үдеткіштің SSL/TLS платасын орнатуға болады.

Хаттаманы кеңейту сипатталған шабуылды жүзеге асыру мүмкін емес, бірақ қайта қарау рәсіміне байланысты барлық ықтимал қиындықтарды шешпейді. Параметрлерді қайта қарау мен бастапқы келісу арасында орын алған ауысым оқиғаларының дұрыс өңделуі, сертификаттың өтуі, кері қайтарылуы және т.б. үшін жауапкершілік қосымшада болады.

2.5 Атака Beast (CVE-2011-3389)

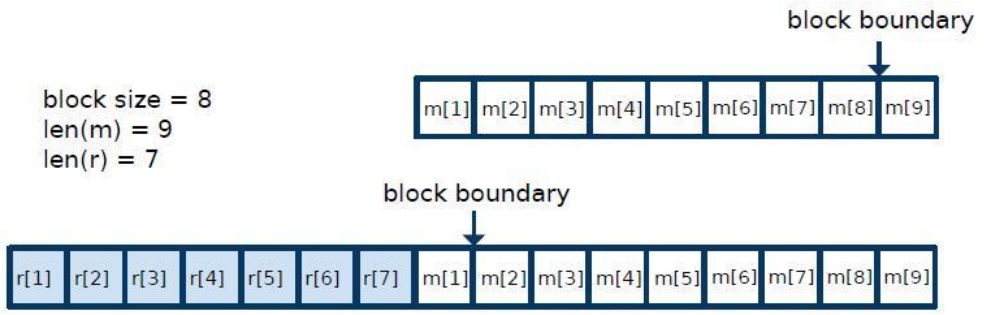
BEAST шабуылдары таңдалған ашық мәтіндермен шабуылдар түріне жатады және блоктардың (CBC, Cipher-block chaining) тіркесу режимінде жұмыс істейтін блоктық шифрларда, SSL 3.0 және TLS 1.0 нұсқаларының хаттамасында бастаушы векторлардың тізбектерін пайдалануға негізделеді. SSL/TLS-де ашық мәтін ұзындығы 214 Байттан аспайтын жазбаларға

бөлінеді, содан кейін әрбір жазба CBC режимінде шифрленеді, онда инициализациялық вектор ретінде (IV) жазу үшін алдыңғы жазба мәтінінің соңғы блогы пайдаланылады. Демек, құрбанның трафигін ұстап тұратын бұзушы шифрлегенге дейін IV келесі жазбаны біле алады. Бұл дегеніміз, бұзушыға блоктық шифрдің кіруін бақылау үшін бірінші блоктың модификациясы жеткілікті. CBC режимінде XOR ашық мәтіннің әрбір блогы соңғы блокпен жазылған мәтін шифры және жаңа блок мәтін шифрын жасай отырып шифрленеді. Бұзушы ашық мәтіннің ізделінетін блогы тең деп болжайды, ал гипотезаны тексеру үшін оған келесі жазбаның бірінші блогы ретінде $-1^{\oplus}$ $-1^{\oplus}$ құрылғыны алу қажет:

$$= (\oplus_{-1}) = (\oplus_{-1}) = \quad .$$

(3.1)

Тәртіп бұзушы үшін ашық мәтіннің барлық блогының ұзындығын таңдаудың қажеті жоқ, ол блоктың басына − 1 байт салып, блокта тек 1 белгісіз байт қалдыру жеткілікті. 2.1-суретте блоктың шекарасын жылжытудың мұндай схемасы көрсетілген. Осылайша, бір байтты ашу үшін бұзушыға 256 әрекет қажет, содан кейін ол сипатталған процедураны келесі белгісіз байттармен қайталай алады және ашық мәтінді қалпына келтіре алады.



Сурет 2.1 - Блок шекарасын ауыстыру схемасы

HTTPS хаттамасы шифрланған байланысты ұсыну және веб-серверді қауіпсіз сәйкестендіру үшін пайдаланылатын HTTP және SSL/TLS протоколдарының комбинациясы болып табылады. HTTPS бөлек хаттама емес, ол шифрланған SSL/TLS сеансында әдеттегі HTTP-ді қолданады. HTTP сұрау келесідей:

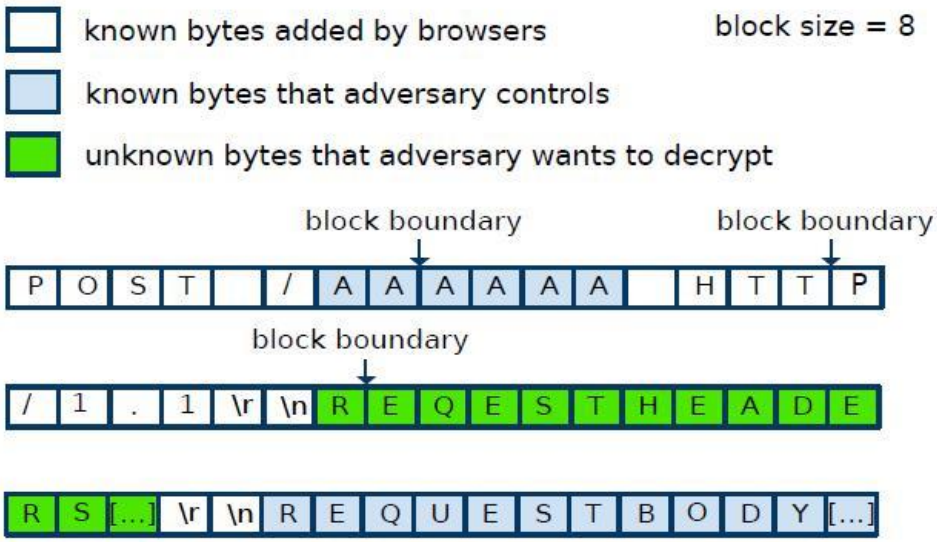
- әдіс, ресурс жолы және HTTP нұсқасы бар сұраныс жолы;
- Session id сияқты сессияны қамтитын тақырып;
- бос жол;
- хабарлама денесі (қосымша).

HTTPS хаттамасында HTTP хабарламасы толығымен шифрланады. Тәртіп бұзушы үшін ең үлкен қызығушылық сеанс идентификаторлары және HTTP тақырыбында қамтылған басқа да cookie. Оларды жаттап, тәртіп

бұзушы құрбанның атынан веб-сервермен операция жасай алады. HTTP шабуылының схемасы төменде көрсетілген (сурет 2.2)

Шабуылдарды жүзеге асыру үшін тәртіп бұзушыға қажет:

- зардап шегушінің пакеттерін ұстау;
- шифрлау кезінде блоктардың шекарасын жылжыту үшін құрбанның браузерінен веб-серверге сұрау салу;
- белгісіз тақырып байттарын таңдау үшін хабар денесіне деректерді қосу.



Сурет 2.2 - HTTP шабуыл схемасы

Бұзушы HTML5 WebSocket API, Java URLConnection API және Silverlight WebClient API көмегімен құрбаны браузеріне агентті іске асыра алады.

2.6 Crime шабуылы

Crime шабуылы ("Compression Ratio Info-leak Made Easy") деректерді қысу алгоритмін пайдалануға негізделген. Клиент пен сервер қорғалған байланыс орнатқан кезде, деректерді шифрлауға дейін, оларды беруді жеделдету үшін деректерді қысу пайдаланылады. Шабуыл жалпы шифрленген байланыс арнасы шеңберінде Cookie ұстап алуды талап ететін сайтқа JavaScript - кодты жалғанған таңбалы деректер блоктарының шифрланған трафигінде бөлу мүмкіндігіне құрылады.

Егер шабуылдаушының зардап шегушінің жағында деректерді қалыптастыру және траффикті бақылау мүмкіндігі болса, онда қысу дәрежесін талдай отырып, шабуылшы өзіне қажетті деректерді байт артынан қалпына келтіре алады.

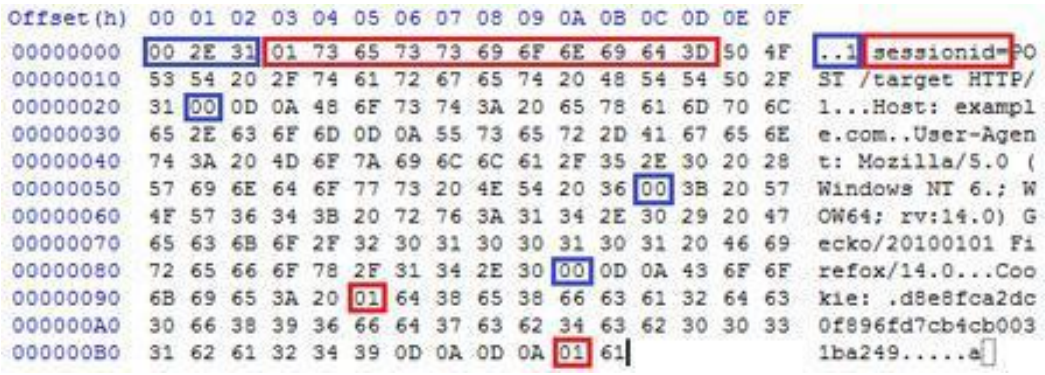
TLS протоколы жіберу үшін хабарды алған кезде, ол оны блоктарға талдайды және қажет болса, сығады, MAC түпнұсқалығының кодын есептеп шығарады, шифрлейді, тақырып қосады және жібереді. Қысу TLS-тің міндетті

функциясы емес, бірақ жиі қолданылады, өйткені ол TLS-ді жеделдетуге арналған.

Бұл мәселе шифрлауға дейін деректерді қысу болып табылады.

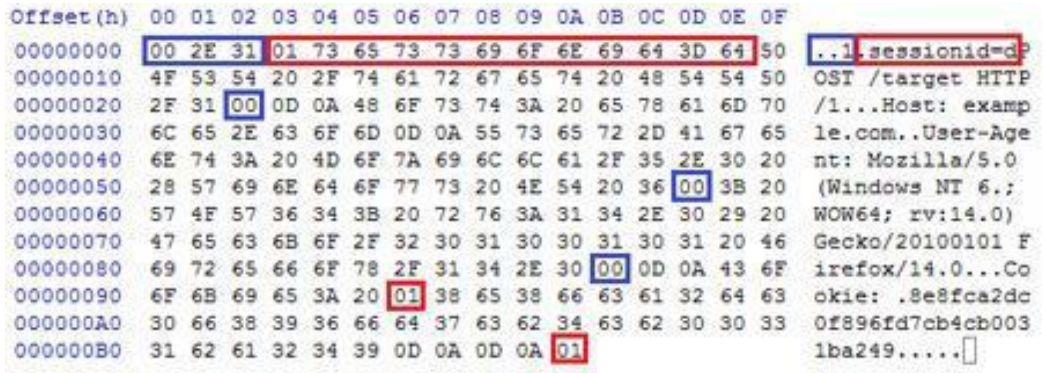
Шабуыл жасау үшін құрбанның компьютеріне деректер мен сұраныстарды айла-шарғы жасайтын зиянды кодты орнату қажет.

TLS хаттамасында Deflate қысу алгоритмі қолданылады, оның негізгі идеясы қайталанатын жолдарды іздеу, оларды сөздікке орналастыру және оларды сөздіктегі тиісті сілтемеге ауыстыру болып табылады. Келтірілген мысалда тек жолдар қайталанады «.1» және «sessionid=» сөздікке орналастырылатын және тиісінше 0x00 және 0x01 қатынасында пайдаланылмайтын байттармен ауыстырылатын. 2.3-сурет қысылғаннан кейін мысал деректерін көрсетеді.



Сурет 2.3 - Сұраудың қысылған деректері

Қысу нәтижесінде деректер көлемі 195-дан 187 байтқа дейін қысқарды. Тәртіп бұзушы 2.4-суретте көрсетілген sessionid=d сәйкестіктерін алғанға дейін бірінші белгісіз байттың аралығын жалғастырады.



Сурет 2.4 – Ашылған 1-ші байтпен сығылғын деректер

Нәтижесінде дұрыс болжанған қысылған деректер 195-тен 186 байтқа қысқарады. Ұсынылған әдістемені қолдана отырып, бұзушы үлкен есептеулерсіз және артық уақыт шығынсыз sessionid шифрланған мәнін ашып, құрбанның атынан серверде аутентификациялай алады.

Crime шабуылы тек TLS көмегімен екі жақтың қысуы мүмкін. Шабуылдарды жариялау кезінде тек Google Chrome және Firefox браузерлері TLS қысуын қолдады, жақында әзірлеушілер TLS қысу қолдауы өшірілген жаңартуды шығарды.

2.7 POODLE шабуылы

Poodle шабуылы ("Padding Oracle On Downgraded Legacy Encryption") екі кезеңнен тұрады. Бірінші кезең - шабуылдаушы клиентке және серверге хаттаманың осал нұсқасымен сөйлесуге мәжбүр болған кезде хаттаманың жоғарғы нұсқаларына арналған. Екінші кезең - шабуылдың өзі.

Poodle шабуыл клиентті хаттаманың төменгі, осал нұсқасын (fallback mechanism) пайдалануға мәжбүр етуге бағытталған. Негізгі мәні - қорғалған қосылым орнатылмаған жағдайда серверлер ескі хаттамаларға ауысады. Қаскүнем SSLv3 пайдалануын таңдай отырып, қосылу қатесін тудыруы мүмкін. Бұл "Downgrade Dance" қағидатымен байланысты (жаңа хаттамалардан ескіге дейінгі хаттамалар нұсқалары бойынша), ол әлі жұмыс істеп тұрған ескі серверлермен жұмыс істеу үшін көптеген TLS клиенттерімен пайдаланылады және керісінше.

Шабуыл жасау үшін қылмыскер құрбанның Интернетке кіруін бақылау мүмкіндігі және құрбанның браузерінде Javascript кодтарын іске қосу мүмкіндігі болуы тиіс.

Хаттама RC4 ағынын шифрлауды немесе CBC режимінде блокты шифрлауды пайдалану мүмкіндігі бар. Шабуылда осы екі алгоритмнің басты мәселелері қолданылады.

RC4-тің басты осалдығы - ығысулардың болуы болып табылады: мысалы, құпия сөз немесе HTTP-cookies сияқты деректерді жіберу үшін көп байланыс пен шифрлау ағындары пайдаланылса, деректерді шифрлеуге болатын Трафиктен көп ақпарат алуға болады. Шифрлеу кезінде CBC шифртекстінің блоктарының ілінісу режимі пайдаланылса, алдымен деректер блоктарға бөлінеді, содан кейін шифрленеді. Барлық блоктар бір ұзындықта болуы тиіс. Сондықтан, блок деректермен толық толтырылмаса, онда бұл блок еркін символдармен толықтырылады.

SSL 3.0-де CBC режимінде шифрлаудың ең маңызды кемшілігі-блоктарды толықтыру еркін болуы мүмкін (соңғы Байттан басқа) және ол имитовставканы есептеу кезінде ескерілмейді. Бұл толық шифрлау кезінде толықтыру тұтастығын тексеру мүмкін емес дегенді білдіреді. 1-ден байтқа дейінгі ұзындықтағы толықтыру, мұнда-байттардағы блоктың өлшемі, CBC режимінде шифрлауды бастамас бұрын блоктардың бүтін санын алу үшін қолданылады. Осалдықты толығымен толықтырудан тұратын блок үшін қолдану оңай: − 1 еркін байт және соңында 1 мәні бар байт. Алынған мәтін шифрын шешу үшін 1, ..., бастамашылық векторы бар 0, мұнда – бір блок, қабылдаушы Тарап 1,..., = () 1 сияқты есептейді, содан кейін толықтыруды тексереді және жояды, және соңында имитовставканы тексереді және жояды.

Егер соңғы блок толық толықтыруды білдіретін болса және шабуылдаушы кез келген ерте блокта сол жазба мәтінінің шифрын ауыстыратын болса, онда мұндай хабарлама қабылданған болады, егер () -1 − ге дейін соңғы байт-1 бар және кері жағдайда қабылданбаса, бұл толықтырулар оракулымен шабуыл жасауға мүмкіндік береді.

Beast шабуылына ұқсас шабуыл әдісін пайдалана отырып: трафикті ұстап қалу және агенттің веб-серверге сұраныстарды жіберу үшін құрбаның браузеріне кірістіру, бұзушы 256 әрекет үшін HTTP тақырыбының 1 байтын ашуға қабілетті. Тәртіп бұзушы ресурстың жолын және HTTP сұрауындағы деректерді өзгертуі мүмкін болғандықтан, шабуылдарды табысты жүргізу үшін талап етілетін шарттар орындалады:

- қосымша барлық соңғы хабарлама блогын толтырады;
- блокта бір белгісіз байтты қалдырып, блок шекарасын жылжыту мүмкіндігі бар.

Блокты блоктармен ауыстыру және модификацияланған жазбаны серверге жіберу арқылы бұзушы сервердің жауаптарын оракул ретінде пайдаланады:

- decryption_failed — пакеттің шифрын тексеру қадамында үзілді-толықтыру дұрыс емес;
- Bad_record_mac-пакеттің шифры имитовставки тексеру қадамында үзілді — толықтыру дұрыс, демек, ізделінген байт ашылады.

2.8 Breach шабуылы

Breach шабуылы (Browser Reconnaissance & Exfiltration via Adaptive Compression of Hypertext) Crime шабуылына ұқсас болып келеді, сонымен бірге, шабуыл Crime шабуылында сияқты SSL деңгейінде емес, HTTP деңгейінде қысу кезінде деректердің ерекшелігіне операция жасайды.

Шабуылшы құрбанның трафиктерін ұстайды. Деректерді қосады және оларды серверге жібереді. Көптеген қысу алгоритмдері ретінде, неғұрлым қайталанатын ақпарат көп болса, соғұрлым ақпарат жақсы қысылады. Яғни, мәтінді қайталау кезінде алгоритм оны қысады. Деректерді серверге жібергеннен кейін шабуылдаушы хабарламаның ұзындығын талдайды. Егер Өлшем азайған болса, онда шабуылшы бірізділікті дұрыс таңдады. Шабуылдаушы жіберетін деректер мазмұнының көп бөлігі белгілі болғандықтан, құпия идентификатор белгісіз (шабуылдаушы сеанс id қалпына келтіруге тырысқан жағдайда), онда жалған сұраныстарды қайта жіберу арқылы шабуылдаушы ізделетін деректердің мазмұнын табудың символына символ ретінде өзінің әрекеттерін қысылған деректердің өлшемін өзгертумен салыстыра отырып, таңбаны алады.

Бұл шабуылды іске асыру кезінде қалған ақпаратты таңдау үшін деректердің бір бөлігін білу қажет.

Шабуылдарды жүзеге асыру үшін, біріншіден, шабуылдаушы трафик үшін бақылау алуы қажет, екіншіден, зардап шегушінің жағында зиянды скрипт болуы қажет. Шабуыл сайтқа зиянды скриптпен жіберілетін

таңбалармен шифрланған трафикте деректер блоктарын бөлу мүмкіндігіне құрылады.

Қосарлы сұрауларды қайта жіберу арқылы, символдың артындағы шабуылдаушы таңбаны, деректерді қысу өлшемінің өзгеруін талдай отырып, деректердің мазмұнын табу.

3 Талдау әдістемесін қалыптастыру

Шабуылдарды талдай отырып, тестілеу әдістемесі негізінде параметрлер мен шарттар жиналды. Әдістеме өзі ережелер жинағы, алгоритм болып табылады. Белгілі шабуылдарды тестілеу әдістемесін жүргізу үшін мен белгілі OpenSSL бағдарламалық құралын қолдандым. Төменде бағдарламаның толық сипаттамасы және таңдалған параметрлер мен шарттардың сипаттамасы берілген.

3.1 OpenSSL бағдарламалық құралы

OpenSSL – это криптографическая библиотека, которая является open source реализацией двух протоколов: Secure Sockets Layer (SSL) и Transport Layer Security (TLS). Данная библиотека имеет инструменты, предназначенные для генерации приватных ключей RSA и Certificate Signing Requests (CSR-запросов), управления сертификатами и выполнения кодирования/декодирования. Библиотека OpenSSL написана на C, однако существуют оболочки для широкого спектра языков программирования.

OpenSSL сертикаттау, шифрлау, хэширлеу көптеген түрлі стандарттарын қолдайды, онда бұл пәрменді пайдалану өте қиын болып келеді. OpenSSL ішінде белгілі бір әрекетке жауап беретін жеке компоненттер бар, қол жетімді компоненттер тізімін алу үшін openssl list-standart-commands параметрлерімен шақыруға болады. Сондай-ақ, қол жетімді хештау алгоритмдері (list-message-digest-commands) және шифрлау алгоритмдері (list-cipher-commands) тізімін алуға болады.

OpenSSL көптеген жағдайларда пайдаланылуы мүмкін және келесі міндеттерді орындай алады:

- RSA және DSA кілттерін құру және басқару-RSA, dsa, dsaparam командалары.
- X509 форматты сертификаттарды жасау, сертификаттауға сұрау салу, қалпына келтіру — X509, req, verify, ca, crl, pks 12, pks7 командалары.
- Деректерді симметриялық немесе асимметриялық шифрлау-enc, rsautl командалары арқылы шифрлау.
- Dgst командасы әр түрлі хештерді есептеңіз.
- S/MIME-мен жұмыс-S/mime командасы.
- SSL серверлері мен клиенттерінің жұмысын тексеру-s_client, s_server командалары.

3.1.1 TLS-пен жұмыс істеуге арналған негізгі OpenSSL командалары

1) TLS сертификаты үшін Кілт жасау.

```
openssl req -batch -noout -new -newkey rsa:2048 -nodes -keyout cert.key
```

Құпия сөзді немесе кілт файлын жоғалтқан жағдайда сертификатты қайта жасау керек.

2) CSR сұрау генерациясы:

```
openssl req -new -key cert.key -out cert.csr
```

Сұраныс жасалған домен аты Common Name - example.com-де жазылады, a challenge password және A optional company name енгізу қажет емес (жай enter басыңыз).

3) кілтті жасау және бір командамен деректер сұрау:

```
openssl req -batch -new -newkey rsa:2048 -nodes -keyout cert.key -subj
'/C=RU/ST=Moscow/L=Moscow/O=Jingel Inc/OU=Research
team/emailAddress=root@example.com/CN=example.com' -out cert.csr
```

4) бір командамен кілт пен өздгінен жазылған сертификат жасау:

```
openssl req -newkey rsa:1024 -nodes -keyout server.key -out server.crt -
x509 -days 3650 -subj \

"/C=XX/ST=XX/L=XX/O=XX/OU=XX/CN=example.com/emailAddress="root@example.c
om
```

5) кілттен парольді алып тастау (сертификат Apache конфигурациясына қолмен қойғанда қажет, әйтпесе ол іске қосылған кезде парольді сұрайды):

```
openssl rsa -in cert.key -out cert.key
```

3.2 Heartbleed-ке тексеру

Сайтты Heartbleed осалдығына тексеру үшін, бірінші кезекте, сервер қолдайтын протоколдың кеңеюін анықтау қажет.

```
for photo in ts1_2 tls 1_1 tls 1 ssl 3; do

Қолдау көрсетілетін сервер кеңейтімдерін $IP адресімен тексеру

В және SSL / TLS-$PORT порты

openssl s_client -connect $IP:$PORT $SDI -$proto-tlsextdebug-
nextprotoneg h2-14,h2-15,h2-status </dev / null 2> $ ERR FILE > $
TMPFILE

нәтижесінде $ TMPFILE файлында қолдау көрсетілетін кеңейтімдер
көрсетілген

хаттаманың әрбір нұсқасы үшін
done
```

Егер қолдау көрсетілетін heartbeat кеңейтімдері тізімінде жоқ болса, онда сервер шабуылға осал емес. Егер сервер кеңейтуді қолдаса, онда сервер қолдайтын протоколдың кез келген нұсқасына ClientHello хабарламасын қалыптастыру және жіберу қажет, және онда heartbeat кеңейту клиентінің қолдауын көрсету қажет. Сервер Hello хабарламасын алғаннан кейін бос heartbeat-пайдалы жүктеменің нөлдік емес ұзындығы бар сұрау жіберуге болады.

Осал сервер жауапта сұралған ұзындықтағы деректерді қайтарады. Осалдығы жоқ Сервер қосылымды қалпына келтіреді. Тестілеу нәтижелері бойынша жоғарыда аталған сайттардан тек бір ғана сайт осы шабуылға осал болды.

3.3 ChangeCipherSpec-ке тексеру

ChangeCipherSpec (CVE-2014-0224) осалдығын тексеру Тараптар сеанс параметрлерін келісу рәсімін орындау кезінде ChangeCipherSpec хабарламасын уақтылы жібермеумен жүзеге асырылады.

Тексеруші серверге ClientHello хабарын жібереді және Server Hello хабарын алғаннан кейін ChangeCipherSpec хабарын жібереді. SMS-хабарламаның бірінші уақытында жіберілмеуіне сервер Unexpected Message қатесімен жауап береді немесе мүлдем жауап бермейді. SMS-хабарламаны екінші жіберу параметрлерді ауыстыру сұрауына decryption failed қатесімен жауап беретін осал серверді анықтауға мүмкіндік береді. Қорғалған сервер Unexpected Message қатесімен жауап береді немесе жауап бермейді, және байланыс өшіріледі.

Мен зерттеу жүргізген сайттарда осы шабуыл анықталған жоқ. OpenSSL бұл осалдықты келесі түрде түзеткендіктен: CCS пакеттер мастер-кілтті орнатқанға дейін алынуы мүмкін емес, ал нөлдік ұзындықтың мастер-кілттері рұқсат етілмейді.

3.4 Сеанс параметрлерін қайта қарау процедурасын тексеру

Сеанс параметрлерін қайта қарау процедурасының қауіпсіздігін тексеру үшін – Secure Renegotiation осалдығы (CVE-2009-3555), SSL/TLS-сервермен байланыс орнату жеткілікті, мысалы:

```
openssl s_client-connect myHost.com:443 | grep 'Secure Renegotiation'
```

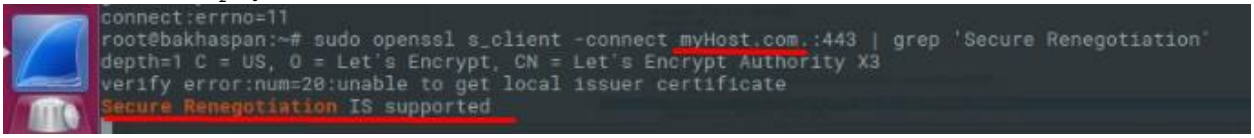
Команданың жауаптарында қайта қараудың қауіпсіз процедурасын қолдауды көрсететін жол бар:

- Secure Renegotiation IS supported-қауіпсіз қайта қарау қолдауы бар, сервер шабуылға осал емес;
- Secure Renegotiation IS NOT supported-қауіпсіз қайта қарауды қолдау жоқ, сервер осал; □

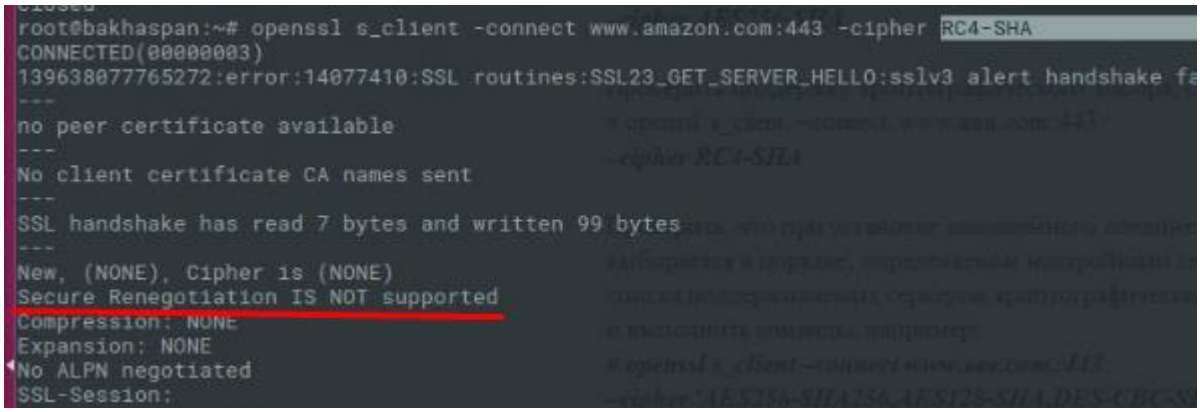
Тексеру нәтижесінің мысалы 3.1, 3.2 - суретте келтірілген. Тестілеу нәтижесі бойынша 3 сайт осы шабуылға осал болды.

Клиент бастамашылық жасаған қайта қарау рәсімін қолдауға арналған серверді тексеру үшін сеанс параметрлерін қайта қарау әрекетін жүзеге асыру қажет:

```
echo R / openssl s_client -legacy_renegotiation-msg-connect myHost.com:443
қайта қарау басталды-NOT ok
```



Сурет 3.1 - Secure Renegotiation шабуылына тестілеу нәтижесі



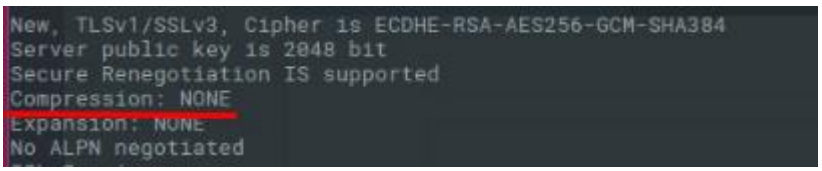
Сурет 3.2 - Secure Renegotiation шабуылына тестілеу нәтижесі

3.5 Crime шабуылына тексеру

Серверді crime осалдығын тексеру үшін онымен SSL/TLS сеанс орнату қажет:

```
openssl s_client –connect myHost.com:443 немесе
openssl s_client –connect myHost.com:443 | grep Compression'
```

Бұдан әрі пәрменнің жауаптарында SSL/TLS деңгейінде қолдау көрсетілетін қысу алгоритмдерін көрсететін Compression жолын талдау. Шабуылдан қорғалған сервер SSL/TLS деңгейінде қысуды қолдамайды және жолда NONE мәні болады. Әйтпесе, сервер TLS-сығуды қолдайды, демек, ол CRIME шабуылына осал. Шабуылдың нәтижжесі 3.3- суретте көрсетілген



Сурет 3.3 - Crime шабуылына тестілеу нәтижесі

3.6 Breach шабуылына тексеру

Серверді BREACH осалдығына тексеру үшін HTTP қысу серверінің қолдауын анықтау қажет-осалдықтың себебі. HTTP қысу қолдауы SSL/TLS сеанс орнатуымен және Клиент қолдайтын қысу алгоритмдерін санамаланған HTTP сұранымын жіберумен тексеріледі.

```
Echo "
GET / HTTP/1.1

Host: myHost.ru
User-Agent: TLS tester
Referer: https://google.com/

Connection: Close
Accept-encoding: gzip, deflate, compress
Accept: text/*\r\n\r\n
```

```
      | ./bin/openssl.Linux.x86_64 s_client -quiet -ign_eof -
connect myHost.com:443
```

Сервердің осал жауаптарында қолданылатын қысу алгоритмін көрсететін Content-Encoding жолы болады. Шабуылдан қорғалған қысу сервері Content-Encoding жоқ жауапты қолдамайды және қайтарады.

Нәтижесінде, мен таңдаған барлық сайттардың ішінен 4 сайт осы шабуылға осал.

3.7 Poodle шабуылына тексеру

Poodle осалдығына серверді тексеру SSL 3.0 протоколы бойынша оған қате имитовкалау және дұрыс емес толықтыру үшін қателердің әр түрлі кодтарын қайтаратын әрекетпен жүзеге асырылады (осылайша, шабуыл үшін қажетті оракул ұсыну арқылы), блоктардың ілінісу режиміндегі шифрлардың бірімен.

```
КДС шифрларды анықтау

cbc_ciphers=$(OpenSSL шифрлары-V Барлығы: null | awk '/ CBC / { print
$1 }' | tr '\N":')

Ssl_v3 БҚ олармен қосылу әрекеті

openssl s_client-sslv3 - $cbc_ciphers шифры - $ NODE IP қосылымы:$PORT-
сервер myHost.com
```

Егер қосылым орнатылса-сервер SSL 3.0 және кем дегенде криптоалгоритмдердің CBC-жиынтығының бірін қолдайды, бұл оның осалдығын куәландырады. Егер сеансты орнату мүмкін болмаса, сервер POODLE шабуылынан қорғалған.

3.8 Beast шабуылына тексеру

Серверді Beast осалдығына тексеру CBC-криптоалгоритмдердің жиынтықтарын пайдалану арқылы қосылуды орнату әрекеттерімен жүзеге асырылады.

SSL 3.0 және TLS 1.0 нұсқаларының хаттамасында алдынғы шифртекст блогының инициализациялық векторы ретінде қолданылатын шабуыл мүмкін етеді.

```
ssl3 tls1 proto үшін; do

хаттаманың көрсетілген нұсқасымен қосылу әрекеті

openssl s_client - "$proto " - $IP қосу:$PORT


егер қосылу мүмкін болса-ПГС жиынтығы тексеріледі

openssl s_client -"$proto" -cipher "$cbc_cipher_list" -connect
$IP:$PORT
done
```

Егер кез келген осал нұсқалар мен жиынтықтарға байланысты орнату мүмкін болса – сервер осал, әйтпесе сервер BEAST шабуылынан қорғалған.

Осылайша, RC4 шифрін қолдамайтын SSL 3.0 немесе TLS 1.0 клиенттерінің байланыс орната алмайтынына көз жеткізу қажет:

```
# openssl s_client –connect www.ввв.com.:443
–no_ssl2 –no_tls1_1 –no_tls1_2 –cipher 'ALL:!RC4'
```

Немесе RC4 шифрін қолдайтын клиенттер оны пайдалана отырып:

```
# openssl s_client –connect www.ввв.com.:443
–no_ssl2 –no_tls1_1 –no_tls1_2 –cipher 'ALL:+RC4'
```

3.9 Қолданыстағы сайттарды талдау

Осы әдістеме бойынша кейбір талаптарға сәйкес 12 қолданыстағы сайтқа талдау жүргізілді. Тестілеу Openssl бағдарламасының және SSlabs бағдарламалық кешенінің көмегімен жүргізілді. Параметрлер, функциялар таңдап алынды және де сайттардың бұл шабуылдарға қаншалықты осал екендігі анықталды.

Кесте 3.1- Талданатын сайттар

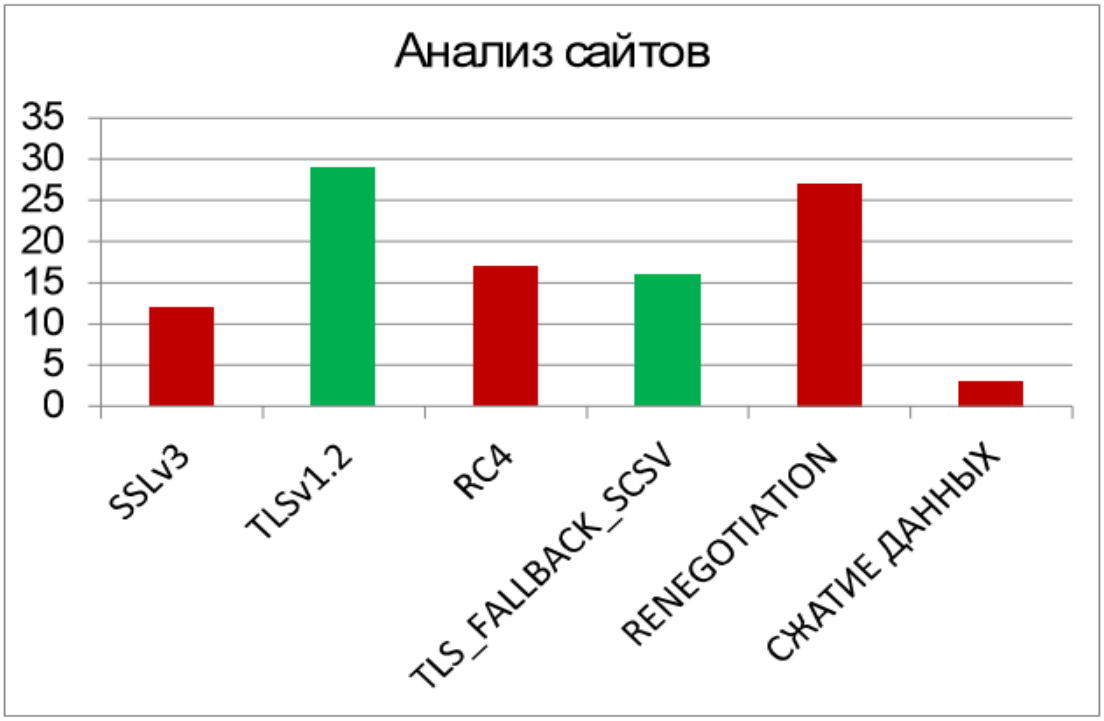
Amazon.com	myHost.com	Vk.com	Ebay.com
Live.com	Twitter.com	Google.com	Toronro.ca
Ugra.ru	Cisco.com	Technet.microsoft.com	Ifmo.ru

4 Тестілеу нәтижелері

Зерттеулер TLS хаттамасының TLSv1.0, TLSv1.1, TLSv1.2 нұсқасында жүргізілді. Ескерту: алдыңғы нұсқада мүмкін болған кейбір шабуылдар белгілі бір шарттар мен реттеулер кезінде жаңа нұсқаларда да мүмкін екені байқалды. Мысалы, Poodle шабуылы TLS хаттамаларында да мүмкін, бірақ бастапқыда бұл шабуыл тек SSLv3 протоколына ғана мүмкін деп бекітілген.

Осы талдауды жүргізгеннен кейін ұсынылған сайттардың жартысы 2015 жылы тыйым салынған осалдықтармен протоколды әлі күнге дейін пайдаланатынына көз жеткізуге болады. Сондай-ақ, бірде-бір сайт BEAST шабуылына ұшырамайтынын байқай аласыз. Құрушының айтуынша, бұл шабуыл теориялық және қиын жүзеге асырылады. Тексерілуші барлық сайттарда RENEGOTIATION механизмі енгізілген, ол шын мәнінде пайдаланушылар үшін өте ыңғайлы механизм, бірақ осал. Бұл сайттар DOS шабуылға ұшырайды. Poodle шабуыл тек SSLv3 пайдаланатын сайттар ғана емес, сондай-ақ TLS қолдайтын сайттар анықталды. Деректерді қысу тек 3 сайтты пайдаланады 12, сондықтан CRIME шабуыл олар ғана ұшырайды. Сайттардың жартысынан көбі пайдалану ұсынылмайтын RC4 шифрлау ағынын қолданады.

Сайт талдауы бойынша гистограмма жасалды (4.1-сурет).



Сурет 4.1 - Сайттарды талдау гистограммасы

Сайттардың шабуылдарға ұшырайтын параметрлері қызыл болып белгіленген.

Келесі гистограммада (4.2-сурет) тексерілген шабуылдарға сайттардың саны көрсетілген.

Сурет 4.2 - Шабуылға ұшыраған талдаудың гистограммасы

4.1 Қорғау жөніндегі ұсыныстар

Тестілеу нәтижелері бойынша ең осал сайттар үшін ұсыныстар жасалды. Ұсынымдарда ықтимал шабуылдарды болдырмау үшін қабылданатын шаралар сипатталады.

Ұсыныс жазылған сайттар келесі кемшіліктердің жиынтығын қамтиды: RC4 ағынын шифрлауды пайдалану, SSLv3 протоколының ескі нұсқасы қолданылады. Сонымен қатар, деректерді қысуды пайдаланатын сайттар.

Осылайша, SSLv3 осы протоколды қолданудан бас тарту және жоғарыда нұсқаларын пайдалану ұсынылды. RC4 арқылы шифрлауды пайдаланатын сайттар RFC ұсынылған басқа алгоритмдерді пайдалану ұсынылады. Қысудан бас тарту ұсынылады.

5 Өмір тіршілік қауіпсіздігі

5.1 Электрмагниттік өрістің адамға әсері

XXI ғасыр – жаңа технологияның, ғылым-білімнің ғасыры. Мұны мойындамасқа шара жоқ. Әрбір әрекет, әрбір жұмыс бір ғана батырманы басу арқылы іске асатын заманға да жақындап келе жатырмыз.

XXI ғасыр-ғылым мен техниканың дамыған кезеңі. Өкінішке орай кез келген өркениеттің екі жағы болатыны бар.Біріншіден, біздің қоғамымыздың алға жылжыуы болса, екінші жағынан, рухани құндылықтарға кері әсерін тигізеді. Біз күнделікті өмірде қолданатын электр құралдардың өз денсаулығымызға қаншалықты зиян келтіретінін кейде білмей де қаламыз.

Электрмагниттік сәулелену дегеніміз (электрмагниттік толқын)-айнымалы электрмагниттік өріс тербелістерінің кеңістікте таралуы (яғни магнит өрісі мен элект өрісінің бір-бірімен әсерлесуі). Магнит өрісі дегеніміз өткізгіштердің электр тогымен өзара әрекеттесуі жүзеге асатын материяның түрі. Электр өрісі дегеніміз кез-келген зарядталған денелердің айналасында пайда болатын, материяның ерекше түрі.

Электрмагниттік сәулелену өзінің көріну жиілігіне қарай инфрақызыл, радиотолқын, көрінетін жарық, ультракүлгін сәулелер, рентгендік және гамма сәулелері. Электрмагниттік сәулелену толқын ретінде таралатындықтан поляризация, толқын ұзындығы және жиілік оның негізгі параметрлері болып саналады.

Электрмагниттік өріс кеңістіктің барлық бағытында $3*10^8$ м/с жылдамдықпен электрмагниттік толқын түрінде тарайды. Жоғарыда айтылған анықтамалар мен ережелер бұл электрмагниттік сәулеленудің физикадағы түсініктемелері. Ал қоғамдағы, күнделікті біздің өміріміздегі электрмагниттік сәулелену дегеніміз ол күні бойына көз алдымызда болатын тұрмыстық техникамен құралдар, қолымыздан түспейтін ұялы телефон және т.б. Сырт көзге байқалмаса да бұлар адам ағзасына белгілі бір мөлшерде зиян келтіруде. [1]

Электрмагниттік толқындар — байланыс тізбегін құрайтын екі сымның арасындағы электрлік және магниттік өрістер бір-бірімен белгілі бір электрмагниттік энергия мөлшерінде байланыста болатын толқын. Күн радиациясы, күннің сәуле шығаруы – Күннің электрмагниттік және корпускулалық сәуле шығаруы.

5.2 Электрмагниттік толқынның әсер ету ортасы

Электрмагниттік толқындар кез келген үйде, мекемеде жалпы адам өмір сүретін барлық ортада бар. Электрмагниттік толқындарды тұрғын үйдің теледидарында, өтегінде, мұздатқыштарында, микротолқынды пеште, шаңсорғыштарда, компьютерде, ұялы телефондарда болады. Электрмагниттік толқындардың 1000 мГц таралу керек болса, электртехникалық құрылғыларда кейде одан көп асып кетеді. Мысалы: өтекті қосқан кезде 25см қашықтықта одан 0,2мкТл электрмагниттік толқындар бөлінеді. «Tefal» шәйнегінде 20см-

0,6мкТл. Кір жуғыш машина 50Гц, ал теледидардың пульті 1 метрде 1мкТл болады. Микротолқынды пеште 30см қашықтықта 50Гц магниттік өрісі 10,3-8мкТл болады. Ал ер адамдар электр қыздырғыш қолданған кезде өздерін әдемілей отырып, беттерінен ток жүргізеді себебі: Электр қырынғыш 100мкТл (микро Тесла) есептеледі екен. Компьютерде 60Гц болады. [2]

Электрмагнитік өрістің әсері – электр заряды не магниттік моменті бар бөлшектер арасындағы электрмагнитік өріс арқылы берілетін белгілі. Адам өмірге келгеннен бастап, электрмагнит сәулесінің әсерінде болады. Адамға, жануарларға, өсімдіктерге, микроорганизмдерге жер қыртысынан бөлінетін гамма сәулелер және ғарыш сәулелері сырттан, организмде болатын радиоактивті элементтер сәуелері іштен әсер етеді. Егер бұл сәулелер тірі организмге артық мөлшерде өтсе, клеткалардың, органдардың тіршілігіне қауіпті ауру жабысады. Радиожиілікті қондырғылар шығаратын электрмагниттік сәулелерді мөлшерден көп қабылдаған жағдайда ол адамда мамандық ауруға әкеліп соғады. Нәтижесінде нерф жүйесі жүрек қан тамырлары эндокриналды жүйе және де басқа да ағзаларға әсер етуі мумкін. Электрмагниттік өріс әсерінде ұзақ уакыт болған жағдайда адамдар тез шаршайды, ұйқышылдық пайда болады, жиі- жиі басы ауырады, нерв жүйесі бұзылады т.с.с. Системетикалық сәулелену болған жағдайда психикалық ауру қан қысымы өзгеру жүрек соғысының баяулауы шашының түсуі байқалады. [3]

Компьютердің электромагниттік толқындардың адам ағзасына тигізер әсері өте көп. Электрмагниттік толқын адамның: жүйкесінің тозуы, себебі компьютерде көп құжат басқан кезде көбісі құжатты сақтауға ұмытып кетеді, кейде жарық өшіп қалады сонда адам стесс алады. «Барлық ауру жүйкенің әсерінен болады» деп айтылған сөз бекер емес. Иммунитет төмендеуі, адам көп отырған кезде қан айналымы бәсеңдейді. Жүктілік кезде, компьютермен жұмыс істеген кезде оның жанында электрмагниттік толқын көп болады. Компьютердің платасы және мониторы қызған кезде ауаға зиян заттар бөлінеді. Осының әсерінен ауа құрғап, адамның тыныс алуы бәсеңдейді. Жүктілік кезде әйел адамның ағзасы көп қимылдағанды қажет етеді. Көп отырған кезде қан айналымы баяулайды, зат алмасу процессі де баяулайды. Жүктілік кезде осының салдарынан гипаксия болуы мүмкін және балаға қажетті заттың дұрыс бөлінбеуіне әкеп соқтырады. Баланың дұрыс дамуына да әсерін тигізеді.

Компьютердің алдында көп отырған кезде басқа да көп аурулар тындауы мүмкін: көз ауруы, қол білезіктерінің ісінуі, омыртқаның қисаюы, салмақтың қосылуы. Осындай ауруларға шалдыққыңыз келмесе компьютердің алдында көп отырмауға тырысыңыз, ал егер жұмысыңыз бойынша талап етілсе арнайы ережелерді сақтап, жаттығу жасап отыру қажет. Компьютер жанына кактус өсімдігін қою қажет. Өз денсаулығыңызға көп көңіл бөлгеніңіз жөн.

Компьютерге осыдан 10 жыл бұрын тек қалталылардыңған қолы жетсе, бүгінгі күні оны әрбір үйден көруімізге болады. Сондықтан болар компьютерлік ойындар балалардың құмартып ойнайтын ойындарының біріне айналды. Қазіргі балалардың досы-компьютер, осы бір жансыз темірдің алдында кешке дейін отырса да жалықпайды. Бұндай балаларды компьютерден басқа еш нәрсе қызықтырмайды.Тіпті кейбіреуі компьютерге тәуелді болады.

Рентген сәулелерінің тірі организмдерге тигізетін залалы мол. Рентгендік сәулелердің өтінде ұзақ болу өте зиян. Теледидар мен компьютер мониторының экрандарына электрондар ағыны соғылғанда да рентгендік сәулелер пайда болады. Мұндай құралдардың қасында өте жақын әрі ұзақ отыру –денсаулыққа нұқсан келтіретінін естен шығармауымыз керек.[2]

5.3 Электрмагниттік өрістен қорғану іс-шаралары

Электрмагниттік өрістің әсері – электр заряды не магниттік моменті бар бөлшектер арасындағы электрмагниттік өріс арқылы берілетіні белгілі. Адам өмірге келгеннен бастап, электрмагнит сәулесінің әсерінде болады. Адамға әсер ететін жердің магниттік өрісі – табиғи электрмагниттік өріс, планетарлық сырқылмайтын ресурс. Магниттік өрістің күші әржерде әртүрлі. Радиожиіліктік өрістер адм организіміне қолайсыз әсерін тигізеді. Адамға, жануарларға, өсімдіктерге, микроорганизмдерге жер қыртысынан бөлінетін гамма сәулелер және ғарыш сәулелері сырттан, организмде болатын радиоактивті элементтер сәулелері іштен әсер етеді. Егер бұл сәулелер тірі организмге артық мөлшерде өтсе, клеткалардың, органдардың тіршілігіне қауіпті ауру жабысады. Радиожиілікті қондырғылар шығаратын электрмагниттік сәулелерді мөлшерден көп қабылдаған жағдайда ол адамда мамандық ауруға әкеліп соғады. Нәтижесінде нерв жүйесі жүрек қан тамырлары эндокриналды жүйе және де басқа да ағзаларға әсер етуі мүмкін. Электрмагниттік өріс әсерінде ұзақ уақыт болған жағдайда адамдар тез шаршайды. Ұйқышылдық пайда болады, ұйқысы бұзылады, жиі-жиі басы ауырады, нерв жүйесі бұзылады т.с.с. системетикалық сәулелену болған жағдайда психикалық ауру қан қысымы өзгеру жүрек соғысының баяулауы шашының түсуі байқалады. Қорғану әдістері: сәуле шығару көзіндегі сәулелenуді азайту. Өте жоғары жиілікті және ультра жиілікті қондырғыларды дұрыс орнату. Экрандалған бөлмелердегі қондырғыны алыстан бақылау. Жұмыс істеу орның және сәуленің шығу көзін экрандау немесе мыстан жасалатын жоғары өткізгіштік қасиеті бар гор металдар шағылдырғыш жерлету экран ретінде пайдалану шаралар “электрмагниттік сәулеленуді дозиметр көмегімен кемінде айыны бір рет тексеру, жылына медициналық тексеруден бір рет өткізу. Қосымша демалыс қысқартылған жұмыс күнін жасау жасы он сегізге толмаған және орталық нерв жүйесі жүрегі көзі ауыратын тұлғаларды жұмысқа қабылдамау ”.

Иондаушы сәулелер әсерінің ерекшеліктері келесідей сипатталады:

- адам сәуленің организмге әсерін сезбейді (адамдар иондаушы сәулелерді қабылдайтын сезім мүшелеріне ие емес);

- иондаушы сәулелер адам денсаулығына зиянды әсерін тигізеді (сондықтан кез келген иондаушы сәулелерді қауіпті деп қараған жөн);

- адам организмінің жеке ерекшеліктері радиацияның аздаған мөлшерінде пайда болады (адам неғұрлым жас болса, соғұрлым сәулеленуге сезімтал болады, 25 жастан бастап дам сәулеленуге тұрақты бола бастайды);

- адам неғұрлым көп мөлшерде сәуле ауруының нышаны, бірақ аурудың нышаны біраз уақыт өткеннен кейін ғана байқалады.

- сәулелену мөлшері жасырын түрде жинақиалады (сәулелену мөлшері уақыт өткен сайын жинақталып, сәуле ауруына ұшыратылады).

Радиациядан қорғанудың үш әдісі бар –олар:

- уақытпен қорғау;

- қашықтықпен қорғау;

- экрандау және жұтып алу арқылы қорғау.

Уақытпен қорғау радио белсенді заттармен ластанған объектіде немесе жергілікті орында адамдардың болуы уақытын шектеу неғұрлым болу уақыты аза болса, соғұрлым қабылданған мөлшер де аз болады.

Қашықтықпен қорғау – радиация деңгейі жоғары немесе жоғарылануы мүмкін жерлерден адамдарды эвакуациялау.

Экрандау және жұтып алу арқылы қорғау – адамдарды эвакуациялау мүмкін болмаған жағдайда қолданылатын әдіс. Бұл әдіспен қорғауда панаханалар, жасырыну орындары және жеке қорғаныс құралдары қолданылады. Тұрғындарды, радиобелсенді заттармен залалдану туралы, төтенше жағдайлар министрлігінің азаматтық қорғаныс органдары хабардар етеді. Жергілікті аймақтың радиобелсенді залалдануы басталған кезінде немесе бірнеше сағатта басталуы мүмкін кезінде Радиациялық қауіп дабылы соғылады. Дыбыс ергілікті радио немесе теледидар желілері арқылы жеткізіледі. Радиациялық қауіп туралы естіген тұрғындар, тез арада бұқаралық ақпарат құралдары бойынша алынған ұсыныстарға сәйкес әс-қимал жасауы керек. Радиациялық сәулелену адам ағзасына және оның дамуына иондық сәулелердің өтуімен кері әсерін тигізеді.[4]

5.4 Операторлық бөлменің жасанды жарықтандырылуын есептеу

Оператордың жұмыс орнының жарықтандыруына көп көңіл бөлінеді. Себебі жарық адам ағзасына әсер етеді. Дұрыс жобаланған жарықтандыру жүйке жүйесінің жұмысын жақсартып,еңбек өнімділігін арттырады. Дұрыс жарықтандырылмаған орында адам нашар жұмыс жасап, тез шаршап, жұмыс кемшіліктері артады.

Жарық, толқынының ұзындығына байланысты қоздыру (қызғылт сары-қызыл), тыныштандыру (сары-жасыл) қасиеттеріне ие. Жарықтың спектральды құрамы жұмыс өнімділігіне әсер етеді. Зерттеулердің көрсетуі бойынша қалыпты жарықтануда адам жұмысын 100% деп алсақ, онда қызыл-қызғылт сары жарықта 76% құрайды.[2]

Жасанды жарықтандыру жүйесі қолданылады: ЛД64-4 люминесцентті шамдар (4 дана).

Бүкіл жұмыс уақыты бойы табиғи жарықтандылу жеткіліксіз, сондықтан жасанды жарықтандыру, яғни люминесцентті шамдарды қолданамыз. 5.1-кестеде күн көзінің түсу нормативі келтірілген.

Кесте 5.1– Ортақ жарықтандыру жүйесіндегі ұсынылған жарық көздері

Түсті ажыратудағы талаптарға сәйкес көру жұмысының сипаттамасы	Жарықтандыру, лк	Күн көзінің түсу температурасының түс диапазоны T_c, °K	Қолданылатын шамдар түрі
Түсті ажырату талаптары көп емес объектілердің түстеріндегі ерекшелігі	500 және ары	3500-6000	ЛБ, (ЛХБ), МГЛ
300, 400	3500-5500	ЛБ, НЛВД+МТЛ	
150, 200	3000-4500	ЛБ, (ЛХБ), НЛВД+МТЛ, ДРЛ	
150 кем	2700-3500	ЛБ, ДРЛ, НЛВД+МТЛ (ЛН, КГ)	

Бұл бөлмеде қалыпты жұмыс жасау жарықтандыруы: 300 лк . Есептеулер төменде көрсетілген.

Қарастырылып отырған офис бөлмесі күн түспейтін жақта орналасқандықтан, жасанды жарықтандыруды қолданамыз. Бөлмеміздің өлшемдері: ұзындығы А = 5 м, ені В = 3,5 м, биіктігі Н = 3 м, төбе ақ, қабырға ашық түсті.

Төбенің еденнен, қабырғадан шағылу коэффиценті сәйкесінше $\rho_п$ = 70% и $p_с$ = 50 %, $\rho_{П=}$ 30%.

Жұмыс жазықтығынан шамның іліну биіктігін есептеу үшін 5.1 формуласын қолданамыз:

$$h_р = H-h_1-h_ж \qquad (5.1)$$

мұнда,

$h_ж$ – шамнан өшіруге дейінгі арақашықтық, $h_ж$=0,8 м ;

h_1– еденнен жұмыс жазықтығына дейінгі биіктік, h_1=0,75 м;

Н – бөлме биіктігі, Н=3 м.

$h_р$=3-0,75 -0,8 = 1,45 м.

Қабырғамен шеткі шырақтар арақашықтығы 5.2 формуламен анықталады:

$$I = A*B/ h_р *(A+B) \quad (5.2)$$

мұнда,

A- бөлме ұзындығы, A=5 м;

B- бөлме ені, B=3,5 м;

$h_р$- жұмыс жазықтығынан шамның іліну биіктігі, $h_р$=1,45.

$$I =5*3,5/1,45*(5+3,5)=1,4$$

есептеуіндегі $p_с$, $p_н$ коэффицентін ескерсек, онда жарықты қолдану коэффиценті η = 0,6. ЛДЦ-80 шамының номинальды жарық ағыны Fл = 2720 лм. Есептей келе шырақ шрақ ағынының 5.3 формуламен анықтаймыз:

$$\Phi = \frac{E\min \cdot S_n \cdot z \cdot K_з}{N \cdot n * \eta} \quad (5.3)$$

мұнда,

E_{min}- ең аз қалыпты жарықтандыру, E_{min}=300;

S_n- жарықтандырылған алаң, S_n=17,5;

z - ең төменгі жарық коэффициенті, z= 1,1;

K_z - қор коэффициенті, K_z=1,5;

N - шамдықтардің саны, N=6;

n - шамдағы шамдардың саны, n=4;

η - жарықты қолдану коэффиценті, η=0,6.

$$\Phi = \frac{300 \cdot 17,5 \cdot 1,1 \cdot 1,5}{6 \cdot 4 * 0,6} = 601 лк ,$$

Қатардағы шырақ санын 6.4 формуламен анықтаймыз:

$$N = E*K*S*z*/n*F_{св}* \eta, \quad (5.4)$$

мұнда,

z- бірқалыпты емес жарықтану коэффиценті, z =1,1;

К –бір жылда екі рет тазалаған кездегі шырақ шаңының қор коэффиценті, К =1,5;

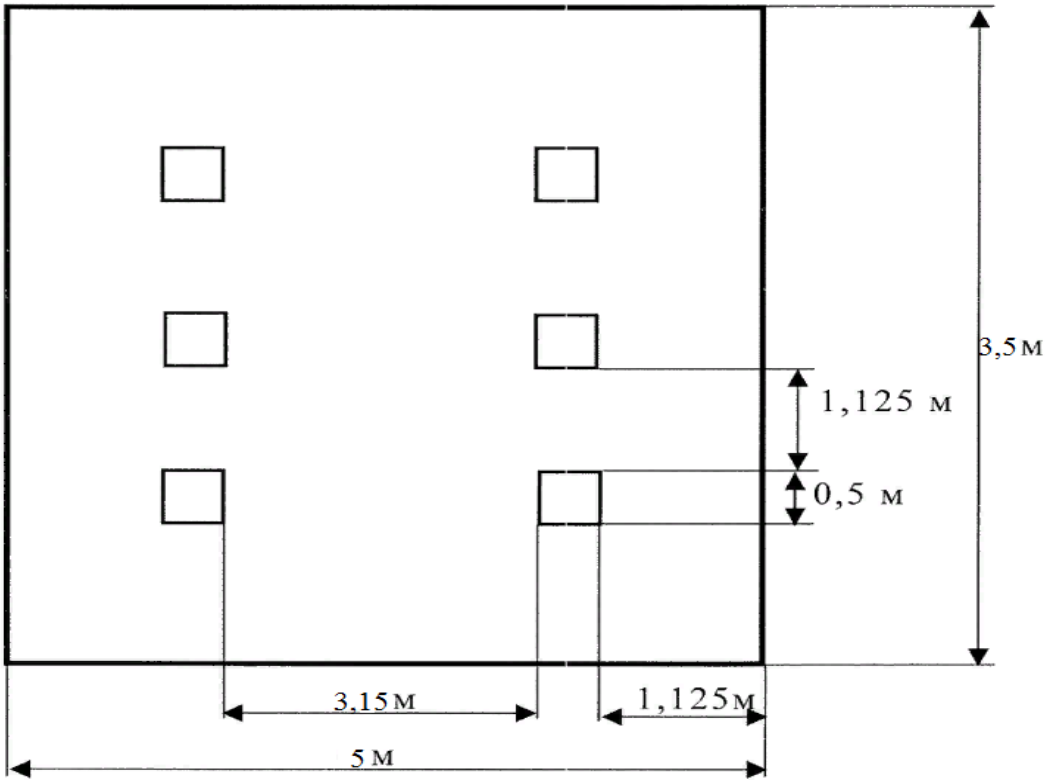
n – шырақ қатарының саны, n=4

Барлық анықталған мәндерді (5.4) формулаға қоя отырып, қатардағы шырақ санын анықтаймыз:

$$N = 300*1,5*17.5*1,1/4*600*0,6 = 6.$$

Барлық есептеулерді ескере отырып, мынадай қорытынды шығаруға болады. 36 кв бөлмені қолайлы жарықтандыру үшін 300 люкс жарық қажет. Ол үшін T8/G13 9Вт 600мм шамы бар, 4 шамды 6 шырақты қолдану керек.

Бөлмедегі төбеде орналасқан шырақтардың орналасу сұлбасы 5.1-суретте көрсетілген:



Сурет 5.1- Оператордың бөлмесіндегі шырақтардың орналасу сұлбасы

(А) Нүктені белгілеп аламыз. Осы нүкте шамдардың суммарлық жарықтандырылуын анықтаймыз.ол үшін А нүктесінен $\mathbf{d_i}$ шамына дейінгі арақашықтықты тауып аламыз. Сосын төбе мен $\mathbf{d_i}$ түзуінің арасындағы бұрышты табамыз. Ол бұрыш арқылы жарықтандыруды есептейміз.

Сонда төмендегі шарт орындалу керек:

$$E_г \geq E_{норм}\ , \tag{5.5}$$

мұндағы

$$E_Г = \Phi \cdot \mu \cdot \frac{\sum_{i=1}^{m} e_Г}{1000 * K_з}\ , \tag{5.6}$$

$$\sum e_{АГ} = \frac{I_\alpha \cdot Cos^3\alpha}{h^2 \cdot K_з}, \tag{5.7}$$

мұндағы

$$\alpha_i = \text{arctg}(\frac{\text{d}_i}{\text{h}})\ , \tag{5.8}$$

орталық нүктеден шамға дейінгі арақашықтық d_i табамыз:

$$d_{1,2,5,6} = \sqrt{0.75^2 + 1^2} = 1.25$$

$$d_{3,4} = 0.75$$

$tg\alpha = \frac{d_{1,2,5,6}}{h_{\text{расч.}}} = \frac{1.25}{1.45} = 0.8$ α = 39^{O} $\cos^3\alpha = 0{,}469$ I= 130 Кд

$tg\alpha = \frac{d_{3,4}}{h_{\text{расч.}}} = \frac{0.75}{1.45} = 0.5$ α = 25^{O} $\cos^3\alpha = 0{,}293$ I= 150 Кд

$$e_{Г1,2,5,6} = \frac{130*0.469}{1.45^2} * 4 = 116.13 лк$$

$$e_{Г3,4} = \frac{150*0.293}{1.45^2} * 4 = 41.85 \, лк$$

$$\sum e_{Гп} = 153.34 \text{ лк}$$

$$E_Г = \frac{600\times1.1}{1000*1.5} * 613.36 = 270.87 \, лк$$

Түйін: Берілген 9Вт қуаттылықтағы T8/G13 лампа саны нормальды жарықтандыруды қамтамасыз етеді, себебі көзбен көру жұмысының III(а) разряды үшін $E_г >= E_н$, Ен = 300 лк орындалады, қателік 10%-ды құрайды.

6 Экономикалық бөлім

6.1 Техникалық-экономикалық негіздеме

Бұл дипломдық жобаның мақсаты TLS көлік деңгейінің протоколын зерттеу болып табылады. Сертификаттарды қорғау бойынша ұсыныстар жасау.

Хаттаманы зерттеуге техникалық жетекші, желілік әкімші кіретін мамандар тобы қатысады. Техникалық басшының міндетіне жұмыс кестелерін сақтау және әзірлеу, оларды бақылау және оңтайландыру кіреді. Жүйелік әкімшінің міндетіне техникалық негіздемені зерттеу, оны тестілеу және сүйемелдеу кіреді. Демек, негізгі жұмыс жүйелік әкімшінің иығына жатады, ал техникалық басшы ұйымдастыру мәселелерімен айналысады. Техникалық-экономикалық негіздеме мынадай тармақтардан тұрады:

- TLS протоколын зерттеу күрделілігін анықтау;
- хаттаманы зерттеуге арналған шығындарды есептеу;
- құндылықты анықтау тестілеу;
- хаттаманы зерттеу нәтижелерін бағалау.

6.2 Әзірлеу күрделілігін анықтау

Протоколды зерттеудің жалпы күрделілігін анықтамас бұрын, барлық міндеттерді бөліп, олар үшін қарапайым кезеңдерді құру қажет. Бұл бізге күрделі міндетті неғұрлым жеңіл беруге бөлу есебінен хаттаманы зерттеудің прогрессті тиімді қадағалауға мүмкіндік береді. Менің көзқарасым бойынша мұндай тәсіл неғұрлым тиімді болып саналады және нәтижелі және тез табыс табуға мүмкіндік береді. TLS хаттамасының тестілеу сатысының курделілігінің моделі 6.1 кестеде көрсетілген.

Кесте 6.1 - TLS протоколын зерттеу кезеңдері

TLS протколын зерттеу кезеңдері	Жұмыс түрі	Еңбек сыйымдылығы, адам сағ.
1 кезең	Міндеттер қою	14
2 кезең		13
3 кезең	Зерттеуге арналған ТТ әзірлеу және бекіту	18
4 кезең	Мұндай зерттеулерді іздеу және зерттеу	12
5 кезең	Ілеспе әдебиеттерді іздеу және зерттеу	24
6 кезең	ҚТҚ платформаларында хаттаманы зерттеу	35
7 кезең	TLS протоколының барлық нұсқаларын зерттеу	30
8 кезең	Белсенді осалдықтарды және хаттама	25

	шабуылдарын іздеу	

6.1-кестенің жалғасы

9 кезең	Осындай шабуылдарға төзімділікке хаттаманы тестілеу	15
10 кезең	Қорытындылау, талдау	23
11 кезең	TLS протоколын қорғау бойынша ұсыныстар жасау	15
Барлығы: зерттеу жобасын орындаудың еңбек сыйымдылығы		224

Жұмыс күнінің ұзақтығы 8 сағатқа тең. Нәтижесінде хаттаманы зерттеуді іске асыру үшін 28 жұмыс күні қажет. (224:8=28)

6.3 Хаттаманы зерттеуге арналған шығындарды есептеу

TLS хаттамасын зерттеу үшін қажетті шығындарды анықтау қолда бар смета негізінде жүргізіледі, ол мынадай элементтерді қамтиды:

- материалдық шығындар;
- еңбекақы төлеу шығындары;
- әлеуметтік салық;
- негізгі қорлардың амортизациясы;
- өзге де шығындар.

Материалдық шығындар TLS зерттеуге қажетті материалдарға, энергияға және басқа да шығындарға бөлінеді.

Материалдық шығындарды есептеу 6.2 кестеде берілген нысан бойынша жүргізіледі.

Кесте 6.2 -Материалдық ресурстарға шығындар

Материалдың атауы	Маркасы	Бірлік өлшеу	Саны	Цена за ед. в тенге	Сумма в тенге
Бумага для офиса	Белоснежка	Упаковка	2	1 300	2 600,00
Тетрадь (96 листов)	Abdi	Штук	3	180	540,00
Блокнот	Abdi	Штук	2	750	1 500,00
Ручки	Abdi	Штук	4	60	240,00
Компьютерная мышь	SmartBuy	Штук	2	3 590	7 180,00
Итого:					12 060,00

TLS протоколын зерттеу үшін Lenovo Ideapad 330 81FK00CXRK Gray ноутбук қолданылады. Ноутбук зерттеу үшін қолайлы сипаттамалары бар, сондай-ақ маңызды артықшылығы Windows 10 x64 орнатылған операциялық жүйесінің болуы және зерттеу үшін қажетті бағдарламалық қамтамасыз ету

болып табылады, жаңа ОЖ және БҚ-ға қосымша шығындар жасау қажеттілігі жоқ.

Материалдық құралдарға (З_м) қажетті жалпы соманы 6.1 формула бойынша есептеуге болады:

$$З_м = \sum P_i * Ц_i, \quad (6.1)$$

мұнда Р_і-материалдық ресурстың і түрінің шығысы, заттай бірліктер;

Ц_і - материалдық ресурстың і түрінің бірлігінің бағасы, тг;

І-материалдық Ресурстың түрі;

n-материалдық ресурстар түрлерінің саны.

Қажетті жабдықтар мен бағдарламалық қамтамасыз ету шығындарын есептеу 6.3-кестеде келтірілген нысан бойынша жүргізіледі.

Кесте 6.3 - Жоба үшін қажетті жабдық пен БҚ шығындарын есептеу

Материалдың атауы	Маркасы	Бірлік өлшеу	Саны	Бірлік бағасы, теңгемен	Сомасы теңгемен
Үздіксіз қоректендіру көзі	UPS/ SVC800/ V-series	Дана	1	26 000	26 000,00
Модем	DELL PowerConnect 7042	Дана	1	22 750	22 750,00
Ноутбук	Lenovo Ideapad 330 81FK00CXRK Gray	Дана	2	320 000	640 000,00
Сервер	Microsoft Windows Server 10 64 bit	Дана	1	100 000	100 000,00
Антивирус	Avast Internet Security	Дана	1	7 500	7 500,00
Бағдарламалық қамтамасыз ету	OpenSSL	Дана	1	5000	5 000,00
Барлығы:					801 250,00

Зм = 12 060 + 801 250= 813 310 (тг)

TLS протоколын жүзеге асыру үшін 813 310 теңге момаға материалдар қажет.

6.4 Электр энергиясына арналған шығындарды есептеу

TLS протоколын зерттеу кезінде электр энергиясын тұтынусыз жүрмейтіндіктен, электр энергиясына кететін шығындарды есептеу мәні бар.

Электр энергиясының құнын есептеу қажет, ол электр энергиясының құнын есептеу қажет, ол 274 сағат ішінде жұмсалады. Оны келесі 6.2 формуламен есептейміз:

$$Э = З_{эл.эн.обор.} + З_{доп.нужды.,} \quad (6.2)$$

мұнда $З_{эл.эн.обор.}$ - жабдықтың электр энергиясына арналған шығындар;

$З_{доп.нужды.}$- қосымша мұқтаждықтарға электр энергиясының шығындары.

Жабдық үшін қажетті электр энергиясын есептеу 6.3 формула бойынша анықталады:

$$З_{эл.эн.обор.} = \sum W * К_{исц} * S * T, \quad (6.3)$$

мұнда W - тұтынылатын қуат, Вт;

$К_{исц}$ - пайдалану коэффициенті ($К_{исц}$ = 0,7-0,9);

Т - жұмыс уақыты;

S – тариф (1 кВт/сағ = 23,85 тг "АлматыЭнергоСбыт" ЖШС заңды тұлғаларға арналған тариф 01.01.19).

Электр энергиясының құнын есептеу бойынша қорытынды 6.4-кестеде көрсетілген.

Кесте 6.4 -Электр энергиясына шығындар

Аспаптардың атауы	Паспорттық қуаты, кВт	Қуат коэффициенті	Жабдықтың жұмыс уақыты, сағ	ЭЭ бағасы тг/кВтсағ	Сомасы, тг.
Ноутбук	0,6	0,7	274	23,85	2744,66
Модем	0,08	0,9	274	23,85	470,51
Үздіксіз қоректендіру көзі	0,6	0,9	274	23,85	3528,85
Жарықтандыру	0,3	0,7	274	23,85	1372,33
Барлығы:					8116,35

$$З_{эл.эн.обор.} = 8116{,}35 \text{ (тенге)}$$

Қосымша қажеттіліктерге шығыстар электр энергиясына арналған шығыстардың 5% көлемінде жоғары көрсеткіш негізінде есептеледі және 6.4 формуламен анықталады:

$$З_{\text{доп.нужды}} = 5\% * З_{\text{эл.эн.обор.}}, \quad (6.4)$$

(6.4) формулаға сәйкес қосымша қажеттіліктерге жұмсалатын шығындарды анықтаймыз.):

$$З_{\text{доп.нужды}} = 0.05 * 8116,35 = 405,82 \text{ (теңге)}$$

Барлық есептеулерге сүйене отырып, электр энергиясына толық шығындар құрайды:

$$Э = 405,82 + 8116,35 = 8522,17 \text{ (теңге)}$$

6.5 Еңбекақы төлеу шығындарын есептеу

TLS протоколын зерттеу үшін екі қызметкер қажет:

- жоба жетекшісі-жұмыс уақытын басқару, жұмыс процестерін түзету, үйлестіру, пәндік облысты зерттеу;
- жүйелік әкімші-зерттеу, тестілеу және сүйемелдеу.

Еңбекақы төлеу шығындарының сомасын 6.5 формула бойынша есептеуге болады:

$$З_{\text{тр}} = \sum ЧС_i * T_i \quad (6.5)$$

мұндағы $ЧС_i$ қызметкердің сағаттық мөлшерлемесі, тг;

T_i - модельді зерттеудің еңбек сыйымдылығы, адам×сағ; і-қызметкердің санаты;

N - TLS зерттеумен айналысатын қызметкерлердің саны.

Жұмыс уақыты әр түрлі, сондықтан әрбір қызметкердің сағаттық ставкасын және жалпы жалақы көлемін белгілеу мағынасы бар.

Қызметкердің сағаттық қойылымын 7.6 формула бойынша есептеуге болады:

$$ЧС_i = \frac{ЗП_i}{ФРВ_i} \quad (6.6)$$

онда $ЗП_i$ - і-ші қызметкердің айлық табыс көзі тг;

$ФРВ_i$ – жұмыс уақытының айлық қоры, сағат.

Басшының айлық жалақысы 350 000 теңгеге тең және жүйелік әкімшінің айлық жалақысы 300 000 теңгеге тең. Әр қызметкердің сағаттық ставкасын формулаға сәйкес есептейміз (6.6):

$$ЧС_{\text{руководитель}} \frac{350\,000}{22 * 8} = 1988,64 \text{ тг/ч}$$

$$ЧС_{сис.\ админ} = \frac{300\,000}{22 * 8} = 1704{,}54\ тг/ч$$

Жоба жетекшісінің сағаттық ставкасы 1988,64 (тг/сағ) құрайды, еңбек сыйымдылығы 100 сағатқа тең. Жүйелік әкімшінің сағаттық мөлшерлемесі 1704,54 (тг/сағ), зерттеудің еңбек сыйымдылығы 274 сағатқа тең. (4.5) формулаға сәйкес қызметкерлердің еңбекақысына арналған шығындар сомасын есептеуге болады:

$$З_{тр} = 1988{,}64 * 100 + 1704{,}54 * 274 = 198\,864 + 467\,043 = 665\,907$$

Еңбек ақы төлеу бойынша шығындарды есептеу (6.5) кестеде көрсетілген.

Кесте 6.5– Жалақыны есептеу

Қызметкердің санаты	Квалификациясы	Еңбек сыйымдылығы, сағ.	Сағаттық ставка, тг / сағ	Сомасы, тг.
Басшы	Инженер-бағдарламашы	100	1988,64	198 864,00
Жүйелік әкімші	Инженер-әкімші	274	1704,54	467 043,00
Барлығы:				*665*907,

6.6 Әлеуметтік салық бойынша шығындарды есептеу

Қазақстан Республикасының Салық кодексіне сәйкес әлеуметтік салық еңбекақы төлеу қорының 9,5% - ын құрайды. Әлеуметтік салықты 6.7 формула бойынша есептеуге болады:

$$С_н = (ФОТ - ПО) * 0{,}095 \qquad (6.7)$$

мұнда ПО-зейнетақы қорына аударымдар, олар ФОТ-дан 10% құрайды.

$$ПО = 665\,907 * 0{,}1 = 66\,590{,}7\ тенге$$

$$С_н = (665\,907 - 66\,590{,}7\ ) * 0{,}095 = 56\,935{,}05 тенге$$

Есептеу нәтижелері кестеде берілген (6.6):

Кесте 6.6 - Әлеуметтік салықты есептеу

Қызметкердің санаты	Адам саны	Айлық табысы, тг	Зейнетақы аударымы, тг	Әлеуметтік салық, тг
Басшы	1	198 864	19 886,4	17 002,87
Жүйелік-әкімші	1	467 043	46 704,3	39 932,17
Барлығы:				56 935,04

6.7 Негізгі қорлардың амортизациясы және өзге де шығындар

Амортизация нормалары ҚҚ анықтау қажет салық кодексіне сәйкес. ОФ амортизациясын 6.8 формула бойынша анықтауға болады:

$$A_{\text{г}} = \frac{\text{С}_{\text{об}} * \text{Н}_{\text{а}}}{100} \quad (6.8)$$

мұндағы, $\text{С}_{\text{об}}$ – жабдықтың құны;

$\text{Н}_{\text{а}}$ - амортизация нормасы (амортизация нормасы = 25);

Формула (6.8) ноутбук үшін бір жыл ішінде амортизациялық аударымдар үшін қажетті соманы есептеуге мүмкіндік береді:

$$A_{\text{г}} = \frac{640\,000 * 25}{100} = 160\,000{,}00\text{тенге}$$

Енді зерттеу кезеңі үшін амортизация нормасын есептеу қажет:

Осылайша, барлық жабдық үшін амортизация нормасын есептеу қажет. Есептеу нәтижелері кестеде келтірілген (6.7).

Кесте 6.7 - ОФ амортизациясы

Жабдық және БҚ атауы	Жабдықтармен БҚ құны, тг	Жылдық амортизация нормасы, %	Жыл ішіндегі амортизация сомасы, тг	Зерттеу кезіндегі амортизация сомасы, тг
Ноутбук	640 000	25	160 000	14 904,11
Үздіксіз қоректендіру көзі	26 000	25	6 500	605,48
Модем	22 750	20	5 687,5	529,79
Антивирус	7 500	15	1 875	174,66
Барлығы:				16 214,04

Хаттаманы зерттеуге арналған шығындар сметасы.

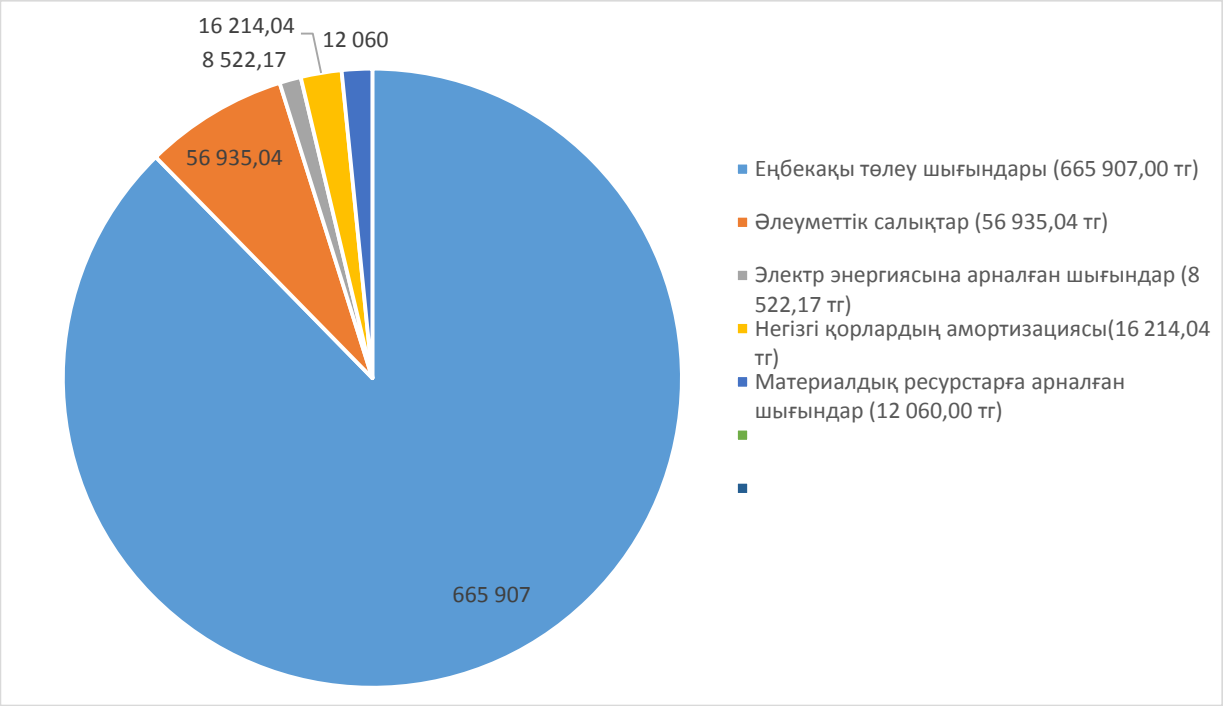
Барлық ұсынылған есептеулер негізінде (6.8) кестеде келтірілген нысанға сәйкес хаттаманы зерттеуге арналған шығыстар сметасын ресімдеу қажет. Суретте 6.1 көрсетілді диаграмма жұмыс шығыстар.

Кесте 6.8 - TLS зерттеуге жұмсалған шығындар сметасы

Шығындар баптары	Сомасы, тг
Жабдыққа арналған шығындар	801 250,00

7.8-кестенің жалғасы

Материалдық ресурстарға арналған шығындар	12 060,00
Еңбекақы төлеу шығындары	665 907,00
Әлеуметтік салықтар	56 935,04
Электр энергиясына арналған шығындар	8522,17
Негізгі қорлардың амортизациясы	16 214,04
Смета бойынша жиыны:	1 560 888,25



Сурет 7.1 – Шығындардың диаграммасы

6.8 TLS зерттеудің ықтимал бағасын анықтау

Хаттаманы зерттеу құны тестілеу, оны зерттеу мерзімі ретінде анықталады. Хаттаманы зерттеу үшін Цдқұнын 6.9 формула бойынша есептеуге болады:

$$Ц_Д = З_{нир}\left(1 + \frac{P}{100}\right), \quad (6.9)$$

мұнда $З_{нир}$ – хаттаманы зерттеуге арналған шығындар, тг;
Р – БҚ рентабельділігінің орташа деңгейі, (%). Бұл параметр 25% тең.

$$Ц_Д = 1\,560\,888{,}25\left(1 + \frac{25}{100}\right) = 1\,560\,888{,}25 + 1\,560\,888{,}25 * 0{,}25$$
$$= 1\,951\,110{,}31 \text{ тенге}$$

Бұдан әрі ҚҚС есебімен сату құнын анықтау қажет, ҚҚС ставкасы ҚР заңнамасымен белгіленеді. 2019 жылға ҚҚС ставкасы 12% құрайды. Іске асыру құны ҚҚС-ты ескере отырып есептеуге болады 6.10 формула бойынша:

$$Ц_р = Ц_д + Ц_д * НДС, \quad (6.10)$$

$Ц_р = 1\,951\,110{,}31 + 1\,951\,110{,}31 * 0{,}12 = 2\,185\,243{,}55$ тенге

Бұл бағаны 2 185 244 теңгеге дейін дөңгелектеуге болады.

Осылайша,

ҚҚС есебімен іске асыру сомасы - 2 185 244 теңгеге тең.

Өзіндік құн - 1 560 888,25 теңгені құрайды.

Пайда - 390 222,062 тг.

Қорытынды

Дипломдық жұмыста TLS протоколының жұмыс принциптері зерттелді. Зерттеудің негізгі мақсаты-TLS протоколын іске асырудың қаншалықты қауіпсіз екендігін анықтау.

TLS протоколының қауіпсіздігін тестілеудің қолданыстағы шешімдерін қарастыру және салыстыру олардың әлсіз жақтарын анықтауға мүмкіндік берді: тестілеу әдістемелерінің толық болмауы, TLS сеанстарын қорғау бойынша ұсыныстарды қалыптастыру және қолдану функцияларының болмауы. TLS протоколының қауіпсіздігін тестілеудің қолданыстағы шешімдерінің кемшіліктері хаттама қауіпсіздігін тестілеудің толық әдістемесін әзірлеуге әкелді.

Протоколды іске асыруды тестілеу әдістемесін әзірлеу мақсатында TLS-ға шабуылдар талданды. Талдау нәтижесінде TLS протоколына ең танымал шабуылдар қатары алынды.

Алынған шабуылдар талданды, осы шабуылдар жүзеге асырылған параметрлер анықталды. Орындалған зерттеу нәтижелері негізінде Хаттаманы іске асыруды тестілеу әдістемесі әзірленді.

Зерттеудің қорытынды кезеңі осалдықтардың, механизмдердің болуына 12 сайтты тестілеу болды, шабуыл сайттары ұшырайды немесе жоқ.

Тестілеу нәтижелері кейбір сайттар шабуылға ұшырайтынын көрсетті. Бұл сайттардың серверлері шабуылшы шабуыл жасай алатындай етіп бапталған.

Осы нәтижелер бойынша кейбір ұсыныстар жасалды. Ұсыныстар осал сайтқа арналады. Онда зиянкестерден қорғауға арналған әдістер мен құралдар сипатталған.

Дипломдық жұмыстың нәтижелері серверлердің қаншалықты қауіпсіз күйге келтірілгені туралы түсінікке ие болу үшін қолданыстағы іске асыруды тестілеудің маңыздылығын көрсетті.

Әдебиеттер тізімі

1. D. Wagner, B. Schneier, “Analysis of the TLS protocol”
2. “Создание фальшивых TLS сертификатов”
3. “Описание протокола SSL/TLS”, URL: https://www.cryptopro.ru/sites/default/files/docs/TLS_description.pdf, 2002. (қолданған мерзімі 02.03.19)
4. Семенов Ю.А. “Алгоритмы телекоммуникационные сетей”, 2004.
5. “Формат сертификатов открытых ключей X.509”, URL: http://www.inssl.com/x509-open-key-specifications.html, 2014. (қолданған мерзімі 25.03.19)
6. “КриптоПро против BEAST”, URL: https://www.cryptopri.ru/blog/2011/12/09/kriptopro-tls-protiv-beast, 2011. (қолданған мерзімі 02.03.19)
7. “Сжатие данных в протоколе HTTP”, URL: http://www.opennet.ru/base/dev/http_compress.txt.html, 2005. (қолданған мерзімі 31.04.19)
8. “TLS Fallback Signaling Cipher Suite Value (SCSV) for Preventing Protocol Downgrade Attacks”, URL: https://tools.ietf.org/html/draft-ietf-tls-downgrade-scsv-00, 2014.
9. “POODLE and the TLS_FALLBACK_SCSV Remedy”, URL: http://www.exploresecurity.com/poodle-and-the-tls_fallback_scsv-remedy/, 2014. (қолданған мерзімі 09.05.19)
10. “Представлена техника перехвата данных для сжатых соединений TLS и SPDY”
11. Методические указания к выполнению раздела «Охрана труда» в дипломном проекте. Алма-Ата,1969.
12. Баклашов Н.И., Китаева Н.Ж., Терехов Б.Д. Охрана труда на предприятиях связи и охрана окружающей среды. – М.: Радио и связь, 1989.-288с.
13. Громов В.И., Васильев Г.А. Энциклопедия безопасности-3 (с изменениями и дополнениями). Москва, 2000.