УДК 004.056

ЖЕКЕ КРИПТОГРАФИЯЛЫҚ ХАТТАМА ҚҰРУДЫҢ ПАЙДАСЫ МЕН ЗИЯНЫ

[1]Қайупов Еркебұлан Керімұлы, [2]Жолдасова Шолпан Шорабековна
[1]yerik.kai@gmail.com
[2]zholdasova.sh@gmail.com
[1]Л.Н. Гумилев атындағы Еуразия ұлттық университеті, Ақпараттық технологиялар факультеті, «Ақпараттық қауіпсіздік» кафедрасының аға оқытушысы, Нұр-Сұлтан, Қазақстан
[2]Л.Н. Гумилев атындағы Еуразия ұлттық университеті, Ақпараттық технологиялар факультеті, «Жасанды интеллект технологиялары» кафедрасының аға оқытушысы, Нұр-Сұлтан, Қазақстан

Аңдатпа. Криптография – бұл ақпаратты қорғауға, шифрлауға және дешифрлауға арналған кеңінен қолданылатын қорғаныс түрлерінің бірі болып табылады. Криптографиялық алгоритмдер желіде қолданылған кезде криптографиялық хаттама аясында жүзеге асырылады. Криптографиялық хаттама-бұл қауіпсіздік тапсырмасын орындау үшін қолданылатын екі тарап арасында орындалатын процедура. Әдетте криптографиялық хаттамадар бір немесе бірнеше криптографиялық примитивтерді және/немесе схемаларын қолданады. Бұл мақалада қауіпсіздік деңгейін қамтамасыз ету үшін жеке криптографиялық хаттама құрудың пайдасы мен зияны жайлы баяндалған.

Кілттік сөздер: криптография, криптографиялық хаттама, ақпараттық қауіпсіздік, TCP/IP, UDP, Https, FTP, POP3, SMTP, TELNET.

Ақпараттық технологиялардың қарқынды дамуы және оның барлық салаларда қолдыла бастауы, оның қауіпсіздік жағын қорғаудың негізіне алып келді. Барлығымыз білетініміздей басында программа жасаса болды деген ұғым қалыптасса, кейінірек барлық адамдардың түсінуі және техникалардың көбеюі немесе интернет желісінің қарқынды дамуы программаларды қорғау қажеттілігін туындатты. Программаны қорғау үшін ең қарапайым интернет желісін қоспаса да болды десек болады. Бірақ мына ақпараттық цифрландыру заманында ол мүмкін емес, ақпарат алмасу керек. Ақпарат алмасу кезінде ақпараттың тұтастығы, құпиялығы, қолжетімділігі толықтай сақталу тиіс.

Ақпаратты қорғау деген кезде автоматты түрде криптография ұғым ақылымызға келеді. Аспан десек көк деген секілді ақпаратты қорғау әдістерінің бірі криптография болып табылады. Ақпарат алмасу үшін көптеген хаттамалар (протокол) қоладылады (hhtp, TCP/IP, UDP, Https, FTP, POP3, SMTP, TELNET). Деректер алмасу хаттамасы – бұл әртүрлі құрылғылар арасындағы мәліметтер алмасуды анықтайтын логикалық деңгей интерфейсінің белгілі ережелері немесе келісімдері, ал желілік хаттама – желіге қосылған екі немесе одан да көп құрылғылар арасында мәліметтер қосуға және алмасуға мүмкіндік беретін ережелер мен әрекеттер жиынтығы (іс-қимылдар тізбегі). Айталық тұтынушы өзінің желілік хаттамасын жасағысы келеді делік. Мысалы, сервер мен мобильді қосымша арасындағы

деректерді беру, микросервистер, программалық модульдер, UDP арқылы немесе TCP арқылы байланыс үшін шифрланған. Неліктен WebSocket және JSON сияқты ашық стандарттарды қолданбасқа, неге жеке хаттама жасау қажеттілігі туады? Әдетте мұның бірнеше себептері бар:

1. Қауіпсіздік үшін, онда реверс инжиниринг (кері инженерия; ағыл. reverse engineering) – кейбір дайын құрылғыны немесе программаны, сондай-ақ оның жұмыс істеу принципін түсіну үшін оған арналған құжаттаманы зерттеу қажет. Мысалы, құжатталмаған мүмкіндіктерді (соның ішінде программалық бетбелгілерді) табу, құрылғыны, программаны немесе осындай функционалдығы бар, бірақ тікелей көшірмесіз басқа объектіні өзгерту немесе көбейту) [1] қолдану қиынырақ болады және сіз қандай деректерді тасымалдайтыныңызды ешкім түсінбейді.

2. Тиімділік үшін. Бізде бірегей пайдалану жағдайы бар, сондықтан стандартты шешімдер оңтайлы болмайды. Біздің жеке хаттамамыз кешігу кезінде жұмыс істейді, өткізу қабілеттілігін аз қолданады және батареяны аз пайдаланады.

3. Себеп – функциялары. Біздің хаттамада, біздің қолдануымыз үшін, біз ашық стандартта немесе бәсекелестерде жоқ ерекше мүмкіндіктерді қолдана аламыз.

Бұл жеке хаттамаларды жасаудың жалпы себептері болып келеді. Кез-келген қауіпсіздік қызметкері хаттама жабық болуы керек дейді. Бұл бәсекелестерден қорғану үшін клиенттерден де маңызды. Клиент хаттама туралы неғұрлым аз білетін болса, соғұрлым ол жүйені, қосымшаны аз басқаруға болады. Барлық мүмкіндік әзірлеушінің қолында болады. Жүйе толығымен өндірушінің бақылауында, яғни сізде деген сөз. Тиісінше, клиент сізге қызмет көрсету үшін үнемі байланысты болады. Ол аппараттық немесе программалық жасақтамада ештеңені бұза алмайды. Жалпы, ол басын сол жаққа жабыстыруға қорқатын болады, өйткені ол жерде ештеңе анық емес. Бәрі бүркемеленіп, шифрланған және түсініксіз тілде жазылған. Мысалы, қызмет көрсету және техникалық қызмет көрсету көптеген компаниялардың ісінің маңызды бөлігі болып табылады. Сондықтан, белгілі бір компания, айталық, жүйелік интегратор клиентке стандартты Open Source шешімдерінің орнына өзінің жеке хаттамасы бар жеке программалық жасақтаманы енгізуді жөн көреді. Кейіннен ол клиент тек сол компанияға ғана тәуелді болып қалады, себебі басқа адам олардың жасаған хаттамасын түсінбейді. Қазіргі кезде нарықта сатып алынатын техника не бағадрлама арзанға түседі, бірақ оған қызмет көрсету қымбатқа соғады. Сондықтан арзанға қызығып, ұрынып қалатын жағдайлар көп кездесіп жатады. Алайда кейбір интеграторлар белгілі бір клиентке арналған бірегей программалық жасақтаманы жазады және өз қызметкерін клиенттік компанияның қызметкерлеріне жібереді. Себебі ол тек осы программамен жұмыс жасауды біледі. Жалпы жеке хаттама фирма үшін тиімді болып көрінгенмен, оның кемшіл тұстары да бар:

1. «Түсінбестік арқылы қауіпсіздік» [2] принципі жұмыс істемейді. Кез-келген хаттаманы реверс инженеринг қалпына келтіруге болады;

2. Меншіктік шифрлау қауіпті болып табылады;

3. Жабық программалық жасақтаманың қателерін жөндеуге сырттан ешкім көмектесе алмайды.

Криптографияда «Түсінбестік арқылы қауіпсіздік» [2] принципі жұмыс істемейді.

Бұлыңғырлық арқылы қауіпсіздік принципі - қауіпсіздікті қамтамасыз ету үшін жүйенің немесе іске асырудың ішкі элементтерін жасыру болып табылады.

Бірақ кез-келген жүйеде кемшіліктер бар. Бұл жағдайда жүйені жасаушы бұл кемшіліктерді жасырғысы келеді, сонда шабуылдаушы оларды пайдаланып кетпейді.

Мұны ашық жүйелерімен салыстырыңыз, мұнда жасаушы кодты әдейі ашады, сонда тәуелсіз бөгде сарапшылар осы кемшіліктерді анықтауға және түзетуге көмектеседі.

Нәтижесінде, жеке хаттама, көзге көрінбейтін көзден мүмкіндігінше жабық, жүйенің қауіпсіздігін мүлде арттырмайды, керісінше төмендетеді!

Криптографияда негізгі ережелердің бірі тек ашық, жалпы алгоритмдер мен хаттамаларды қолдану болып табылады. Мұндай жүйеде бір ғана құпия бар – жеке кілт.

Одан басқа ештеңе болмау керек. Бұл криптографияда кеңінен қолданылатын және сөзсіз дерлік болып саналатын Керхофс принципі [3].

«Неге өз криптографиясын дамытпасқа?» деген сұрақ туындайды. «Неліктен ұшақтың қозғалтқышын жасамасқа?» деген сұраққа ұқсас, қауіпсіздік техникасын зерттеуші Руна Сандвик айтады. Әрине, біз мұны теория жүзінде жасай аламыз. Бірақ бұл өте қиын. Біршама қарапайым және сенімді нұсқа – дайын шешімді, дәлелденген және сенімді хаттамалар мен алгоритмдерді таңдау болып саналады.

Сондықтан, егер компания өзінің жеке хаттамасын қолданса, бұл ақпараттық қауіпсіздік қауымдастығында өте күдікті. Мысалы, Telegram-ның меншікті MTProto хаттамасына алғашқы кезде көптеген сын-пікірлер жазылды. MTProto 1.0-ны бұзу 2013 жылы Хабредегі ең танымал мақалалардың бірі болды: «Telegram қауіпсіз бе? немесе MTProto-дан бетбелгіні қалай іздедім» (спойлер: меншікті криптографиядағы ақымақ қателер).

Сонымен қатар, мессенджерде телефон нөмірінсіз жасырын тіркеуге тыйым салынады – бұл коммерциялық компания үшін спамды бұғаттап, қосымшаны мекен-жай кітапшаларында насихаттауға ыңғайлы болуы мүмкін. Миллиардтаған пайдаға қауіп төніп тұрғанда, жасырындықты кім ойлайды? Сонымен қатар, Telegram бастапқыда «қауіпсіз» мессенджер ретінде орналасты (көптеген пайдаланушылар осындай жарнаманы сатып алды).

Шындығында, жасырын болуды қамтамасыз ету үшін сіз жасырын SIM картасымен тіркелуіңіз қажет, алайда бәрі мұндайды түсіне бермейді. Телеграммадағы аккаунтты қалай қорғауға болатынын және Интернеттегі анонимділіктің практикалық нұсқауын қараңыз.

Телефон нөміріне байлану пайдаланушыны осал етеді, өйткені ел ішіндегі ұялы байланыс операторлары арнайы қызметтердің жұмысына ыңғайлы объект болып табылады.

Әрине, ашық дереккөздің өзіне тән тәуекелдері болады. Айталық, сіз басқара алмайтын жүздеген тәуелділікке қатысты мәселелер. Мысалы, GitHub-тағы жобалардағы қателіктердің 20% -ы қасақана ниетпен жобаларға әдейі енгізілген. Яғни, қасақана әрекет еткен зиянды салымшылар. ESLint сервері туралы әңгіме әлі ұмытылған жоқ, ол eslint-kapsam және eslint-config-eslint пакеттерінің зиянды нұсқаларын 2018 жылдың 12 шілдесінде npm репозиторийінде жариялады.

Сондықтан, кейде олар өз жобаларын сатуға келіседі (шолғыш кеңейтімдерімен бірдей оқиға). Бұл жоба мыңдаған адамдарға тәуелділік ретінде жүзеге асырылып үлгерді. Бірақ қауіпсіздікке қатысты барлық мәселелер шешіледі. Кәсіби сарапшылардың ашық көзге тәуелсіз аудиті оның сенімділігінің ең жақсы кепілі болып табылады.

Өткен ғасырда меншікті программалық жасақтаманы кәсіпқойлар, ал ашық көзді әуесқойлар жазады деп сенген. Бүгінгі күні ашық бастапқы программалардың кәсіби деңгейі меншіктікінен кем түспейді. Мүмкін олардан да асып түсетін шығар. Жалпы ақпараттық өрбу болу үшін тек қана дайын жүйелерді оптимизациялай бермей, жаңа алгоритмдік жүйелерді ойлап тапқан жөн деп ойлаймыз, егерде мемлекетке қауіп тудыратындай жағдай болмаса. Тек қана эксперименттік әрекеттер ғана жаңа заттар туғызады.

Қоланылған әдебиеттер мен желілік сілтемелер

1. Бирюков А.А., Информационная безопасность: защита и нападение. – М.:ДМК Прес,2016, 422с.
2. https://ru.wikipedia.org/wiki/обратная разработка
3. https://en.wikipedia.org/wiki/Security_through_obscurity
4. https://ru.wikipedia.org/wiki/Kerckhoffs%27s_principle