ӘОЖ 004.032.97

БАЙЛАНЫС ЖЕЛІЛЕРІНІҢ ҚАУІПСІЗДІГІ ЖӘНЕ КРИПТОГРАФИЯЛЫҚ ЖҮЙЕЛЕР

Нұртаза Қожанберді Нұртайұлы
Л.Н.Гумилев атындағы ЕҰУ-нің 3-курс студенті, Астана, Қазақстан
Касенова Мерейлим Нурлановна
Техника ғылымдарының магистрі, Радиотехника электроника и телекоммуникациялар кафедрасының оқытушысы

Желі қорғанысын қамтамасыз етудің бірнеше тәсілдері бар. Желілер желіге кіруді басқару тізімдерімен, мәліметтерді сәйкестендірумен (аутентификация), авторизация және тіркеумен (AAA), брандмауэр функцияларымен және рұқсатсыз желіге енуді тоқтату (IPS) жүйелерімен қорғалуы мүмкін. Бұл функциялардың бірлесе жұмыс жасауы нәтижесінде жергілікті желінің инфрақұрылымы және соңғы құрылғылары қорғалады. Бірақ, желілік трафик жалпыға ортақ Интернет желісінсіз қалай қорғалған? Жауабы – криптографиялық тәсілдер арқылы.

Криптологияның жұмыс жасау принциптері арқылы заманауи протоколдар мен алгоритмдердің жеке хабарламаларды қорғау үшін қалай қолданылатындарын түсіндіруге болады. Криптология – аса құнды ақпараттарды қорғауды қаматамасыз ету үшін жасырын кодтарды жасап шығару және осы жасырын кодтардың кілттерін анықтауды зерттейтін ғылым. Құпия кодтарды жасап шығару мен оларды қолдану криптография, ал үзілім кодтары криптоталдау деп аталады. Криптография ғасырлар бойы құпия құжаттарды қорғауға қолданылып келеді. Мысалы, Юлий Цезарь ұрыс кезінде өз қолбасшыларына хабарламаларды қауіпсіз жіберу үшін қарапайым әліппелік шифрді кеңінен қолданған. Ал қолбасшылар өз кезегінде хабарламаны дешифрлеуге қажетті кілтті біліп отырған.

Шифрлеу кодының жасап шығарылуы

Криптографиялық жүйелердің тарихы мың жыл бұрынғы дипломатиялық шеңберден негіз алады. Шифрленген хабарламаларды ең бірінші болып әскери қолбасшылар қолдана бастады.

Ғасырлар бойы ақпарат қауіпсіздігін қамтамасыз ету үшін шифрлеудің түрлі тәсілдері, көптеген құрылғылар мен құралдар кеңінен қолданылып келді:

- Scytale;
- Цезарлық шифр;
- Виженер шифры;
- Энигма машинасы.

Шифрлеудің бұл тәсілдерінің әрқайсысы ақпаратты шифрлауға немесе шифрын анықтауға арналған арнай алгоритмді қолданады. Шифр ретінде анықталған қадамдар қатары орындалады. Шифрленген мәтінді құрудың бірнеше әдістері бар:

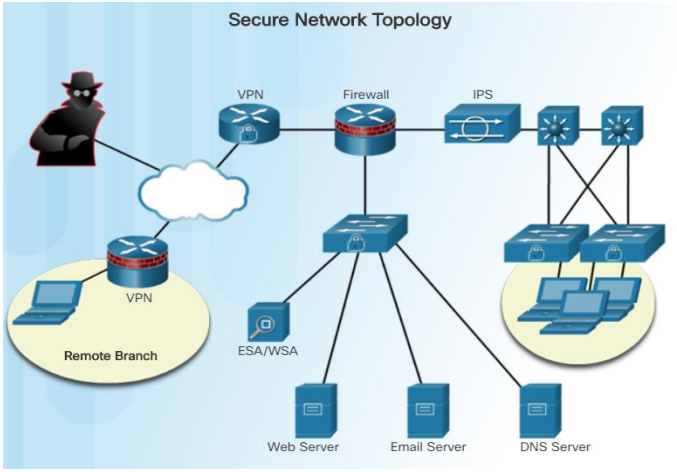
- Қайта орналастыру;
- Алмастыру;
- Бір реттік панель.

Қазіргі таңда, криптографиялық әдістер желінің қауіпсіздігін қаматамасыз ету үшін сан алуан түрде қолданылады.

Сәйкестендіру (аутентификация), деректер тұтастығы, деректердің құпиялылығы

Мемлекеттік және жеке инфрақұрылымдардың қауіпсіздігін қамтамасыз ету үшін желілік администратордың ең бірінші мақсаты желілік инфрақұрылымның қауіпсіздігін қамтамасыз ету болып табылады. Сонымен қатар, маршрутизаторлар, коммутаторлар, серверлер және хосттардың да қауіпсіздігі қамтамасыз етілуі қажет. Мұндай қауіпсіздік шараларын құрылғыларды күшейту, AAA көмегімен байланысты басқару, ACL тізімдерін, брандмауэрлерді, IPS технологияларын қолданумен қауіпсіздік мониторингін жүргізу арқылы, Advanced Malware Protection (AMP) көмегімен соңғы құрылғылардың қауіпсіздігін

қамтамасыз ету және Cisco Email Security Appliance (ESA), Cisco Web Security Appliance (WSA) арқылы жеке электронды поштаның қауіпсіздігін және веб қауіпсіздікті қамтамасыз етуге болады. Суретте қорғалған желінің желінің сұлбасы көрсетілген.



Сурет 1 – Желі қауіпсіздігінің топологиясы.

Келесі мақсат – көптеген бағыттарға бағытталған ақпараттардың қауіпсіздігін қамтамасыз ету. Қауіпсіздікті қамтамасыз етудің бұл сатысындағы ең басты мәселе – инфрақұрылымның сыртында орналасқан филиалдарға, серіктес құрылымдардың сайттарына жіберілетін ақпараттың қауіпсіздігі.

Байланыс қауіпсіздігін қамтамасыз етудің үш негізгі мақсаты бар:

Сәйкестендіру (аутентификация). Хабардың жалған емес екендігі және шын мәнінде кімнен жіберілгені туралы кепілдіктер.

Деректер тұтастығы – ақпараттың басқа біреумен ұрланбағандығына және өзгертілмегендігіне кепіл береді.

Деректердің құпиялылығы. Ақпарат ұрланған жағдайда ақпараттың құпия шифрсыз оқылмайтындығына кепіл.

Көптеген заманауи желілер ақпаратты аутентификациялауды хэш хабарламалардың аутентификация коды (HMAC) сияқты протоколдар көмегімен жүзеге асырады. Деректер тұтастығы MD5 немесе SHA алгоритмдерінің орындалуы арқылы сақталады. Деректердің құпиялылығы симметриялы шифрлеу алгоритмдері, ақпараттарды шифрлеу стандарты (DES), 3DES және ақпараттарды кеңінен шифрлеу стандарты (AES) арқылы іске асырылады. Симметриялы шифрлеу алгоритмдері алдын ала шарт қою арқылы жұмыс жасауға негізделген. Осылайша, ақпаратты жіберуші жақ пен қабылдап алушы жақтар шифрлеу кілтін алдын ала біліп отырады. Декретердің құпиялылығы сондай-ақ Rivest, Shamir және Adleman (RSA) сынды асимметриялық алгоритмдер арқылы және ашық кілт инфрақұрылымы (PKI) сынды технологиялармен де қамтылуы мүмкін. Асиммертриялық алгоритмдердің жұмыс жасау принципі бойынша ақпарат алмасушы жақтар шифрлеудің кілтті сөздерімен алмасу үшін де қауіпсіз тәсілдерді пайдаланады.

Аутентификация. Желілік байланыс барысында келіп түскен ақпарат көзінің жалған емес екендігін тексерудің негізгі екі тәсілі бар: аутентификация қызметтері және ақпараттарға рұқсат бермеу қызметтері.

Аутентификация ақпараттың көрсетілген ақпарат жіберушіден келгендігінің кепілдемесі. Аутентификацияның жұмыс принципі банктік қызмет көрсету үшін банкоматқа еңгізілетін жеке идентификаторлық номерге (PIN) ұқсайды. Идентификаторлық номер жеке тұлға мен финанстік мекеме арасындағы ақпарат алмасуға жалған ақпарат көздерінің енуіне жол бермейді. Байланыс желілерінде аутентификация криптографиялық тәсілдерді қолдана отырып орындалуы мүмкін. Аутентификацияда криптографияның қолданылуы электрондық

пошта немесе IP сияқты және басқа да қосымша протоколдарда өте маңызды. Себебі мұндай қосымшаларда ақпарат көзінің жалған ақпарат көзімен ауыстырылуына жол бермейтін механизмдер жоқ.

Ақпараттардың үзіліссіздігі – аутентификация қызметі сияқты ақпаратты жіберушіні сәйкестендіретін технология түрі. Аутентификация және ақпарат үзіліссіздігі технологиялары өзара бірдей қызмет атқаратындай болып көрінуі мүмкін. Екі технологияның да қызметі ақпарат жіберушіні анықтау болып табылғанымен екі механизм арасында айырмашылық бар.

Ақпарат жіберуші ақпаратты жібергенін жоққа шығара алмайды. Егерде ақпарат жіберілген болса, онда міндетті түрде ақпаратты жіберуші жайлы белгілі болады. Ақпаратты жіберуші ақпаратты өзі жібергенін растау үшін, мағлұматты түрлендіреді. Мұндай түрлендіру тек ақпарат жіберушіге тән. Ақпаратты қабылдап алушыға ақпараттың қалай өңделгені жайлы белгісіз болады. Осылайша, желі ішінде ақпарат көзі қай құрылғы екендігі айқын белгілі болады. Ал ақпарат қабылдаушы құрылғы ақпарат жіберуші ретінде ешқандай жалған операциялар орындай алмайды.

Деректер тұтастығы. Деректер тұтастығы ақпаратты тасымалдау барысында, ақпараттың мүлдем өзгертілмейтіндігіне кепіл болады. Деректер тұтастығы кезінде ақпаратты қабылдап алушы жіберілген ақпарат пен қабылданған ақпаратты салыстыра отырып, ақпаратқа өзгертулер еңгізілгені немесе тұтастық сақталғанын тексере алады.

Еуропалық отбасылар, мемлекеттік қызметкерлер, әскери қызметкерлер, жоғары лауазымды тұлғалар хат салынған конвертті тұтастығын сақтау үшін балауыздан жасалған мөрлерді пайдаланған. Мөр көп жағдайда сақиналар арқылы басылған. Ал сақина әрдайым өз иесінің қолында тағылып жүрді.

Егер мөр бұзылмаған болса, ақпараттың тұтастығы сақталды дегенді білдіреді. Сондай-ақ, конвертке басылған мөр хаттың шынайы екендігінің дәлелі болды.

Сурет 2 - Деректердің құпиялылығы.

Деректердің құпиялылығы ақпаратты тек қабылдап алушының ғана оқи алуын қамтамасыз етеді. Ол үшін жіберілетін ақпарат шифрланады. Ақпаратты шифрлау – ақпаратты бөгде біреу оқи алмауы үшін ақпаратты скремблерлеу процесі.

Шифрлеу кезінде өзгертілетін ақпарат ашық ақпарат деп, ал ашық ақпараттың кері шифрленген түрі шифрленген ақпарат деп аталады. Ақпараттың ашық түрі шифрленген түрге айналған кезде, бөгде адам ақпаратты оқи алмайды. Шифрленген ақпаратты қайтадан ашық түрге айналдыру үшін шифрлеу кілті қажет болады. Шифрлеу кілті – бұл ашық ақпарат пен шифрленген ақпарат арасындағы байланыс.

Хэш-функцияларды пайдалану – деректердің құпиялылығын сақтаудың тағы бір әдісі. Хэш-функция символдар қатарын қысқа мағыналы шамаға немесе тікелей шифр кілтіне айналдырады. Ақпаратты шифрлеу мен хэш-функцияның айырмашылығы ақпараттың сақталу түрінде. Шифрленген ақпаратты шифр кілтінің көмегімен қайтадан ашық ақпаратқа түрлендіруге болады. Хэш-функция технологиясы пайдаланылған кезде

еңгізілген ақпарат түрленеді және ашық ақпарат ретінде жоғалады. Мысалы, желі қызметтерін қолданушы құпия сөзді еңгізетін болса, құпия сөз хэшталады және алдын еңгізіліп хэшталған шамамен салыстырылады. Егерде қолданушы құпия сөзді ұмытып қалған болса, хэшталған құпия сөзді қайтадан ашық ақпарат түріне келтіру мүмкін болмайды.

Екі технологияның бір-бірінен айырмашылығы бар болғанымен мақсаттары бірдей – ақпараттың құпиялылығын сақтап қалу.

Криптографиялық шифрлеумен қатар әрдайым криптоанализ де қолданылатын болады. Криптоанализ – шифр кілтін қолданбай шифрленген ақпараттың мағынасын анықтауға арналған зерттеулер.

Криптоанализде бірнеше тәсілдер кеңінен қолданылады:

–Қарапайым әдіс. Шифрленген ақпараттың кілтін табу үшін мүмкін болады деген барлық нұсқаларды байқап көру. Ең соңында қойылған нұсқалардың біреуі сәйкес келуі тиіс.

–Шифрланған мәтін әдісі. Шифрланған ақпараттың бірнеше мәтіндері бар және ашық ақпарат болмаған жағдайда, кілт сөзді табуға тырысу.

–Қарапайым мәтін әдісі. Шифрланған және ашық ақпараттың көшірмелері болған жағдайда, ақпарат түрлерін салыстыру арқылы кілт сөзді табуға тырысу.

–Примечание. Подробная информация о том, как эти методы реализованы, выходит за рамки этого курса.

–Қарапайым мәтіннен таңдау әдісі. Шифрленетін ақпаратты біле тұрып, шифрлену процесін бақылау.

–Шифрленген мәтінді таңдау тәсілі. Әртүрлі шифрленген ақпараттарды ашық ақпаратпен салыстыру арқылы таңдау.

–Ашық ақпараттың бөлігін біле отырып, шифрленген ақпарат арасынан белгілі бөлікті тауып, кілт сөзді табуға тырысу.

Қолданылған әдебиеттер тізімі

1. Лоренс Б. Novell NetWare 4.1 в подлиннике СПб: BHV, 1996.
2. Ресурсы Microsoft Windows NT Server 4.0 СПб: BHV, 1997.
3. Сетевые средства Microsoft Windows NT Server 4.0 СПб: BHV, 1997.
4. Олифер В.Г., Олифер Н.А. Компьтерные сети, принципы, технологии, протоколы. СПб: Питер, 2000.

ӘОЖ 621.391.037.3

ARDUINO МК ПАЙДАЛАНЫП, ПИАНИНО ДЫБЫСЫН ШЫҒАРУ ЖӘНЕ ДЕ АЛЫНҒАН НӘТИЖЕНІ ТЕХНОЛОГИЯҒА ИКЕМДЕУ

Рахман Ұлжалғас, Әбдіраман Назгүл
Л. Н Гумилев атындағы Еуразия ұлттық университетінің студенттері
Ғылыми жетекшісі – РЭТ кафедрасының профессоры Әубәкір Дәуренбек Әзенұлы

1 ҚҰРЫЛҒЫНЫ ҚҰРАСТЫРУ

Құрылғының жұмыс істеу қағидасы: сенсорлардың әрекеті кілттердің көлемін өлшеуге негізделген, ол бізбен сенсор арқылы өзгереді. Әрбір кілттің Arduino тақтасында өз шығарылымы бар. Сондай-ақ, бір шығу барлық кілттер үшін ортақ және біреуі үшін динамик үшін пайдаланылады. Бұлай дегеніміз, егер бізде 20 штепсельдік тақта бар болса, оның 14-і цифрлық және 6-аналогтық болса, 20 пернесі бар фортепиананы құруға болады. Егер сізде Arduino Mega немесе басқа да штепсельдер көп болса, сіз көп кілтпен жасай аласыз!

1-қадам: Кілттеріңізді жасаңыз