**Дәріс № 15. М2М желілерінің қауіпсіздігі. М2М желілерінің қауіпсіздігін қамтамасыз ету әдістері. М2М желілерінің қауіпсіздік жүйесінің архитектурасы**

Мақсаты: М2М желілерінің қауіпсіздігін қамтамасыз ету мәселелері мен әдістерін зерделеу, М2М желілерінің қауіпсіздік жүйелерінің архитектурасын құру.

M2M желілерінің қауіпсіздігіне қауіптер. M2M құрылғылары мен желілері жұмыс істеудің, тарифтеудің, орналастыру және пайдалану шарттарының бірегей ерекшеліктеріне ие. M2M құрылғылары, әдетте, кішкентай болуы керек, құны төмен және ұзақ уақыт бойы адамдардың бақылауынсыз жұмыс істей алады, сонымен қатар деректерді сымсыз Ғаламдық немесе жергілікті желілер арқылы жібереді. M2M құрылғылары көбінесе адамның күш-жігерінсіз орнатылады және әдетте олардың функцияларын қашықтан басқаруды қажет етеді. Олар сондай-ақ қызметтерді белсендіруді басқару тұрғысынан икемділікті талап етеді. Сонымен қатар, кейбір M2 m қосымшалары үшін көп мөлшерде қолданылады

M2M құрылғылары және олардың көпшілігі мобильді болады. Бұл олардың физикалық қызметін өте ауыр етеді.

M2M құрылғылары мен желілерінің жұмыс істеу ерекшеліктері олардың қауіпсіздігіне бірқатар ерекше қауіп төндіреді, оларды келесі санаттарға бөлуге болады [30-33]:

- Физикалық шабуылдар: заңсыз сәйкестендіру модульдерін M2M құрылғыларына қосу (Machine Communication Identity Module, MCIM), M2M құрылғыларына алаяқтық бағдарламалық жасақтаманы орнату, сондай-ақ M2M құрылғыларына механикалық әсер ету, олардың зақымдалуына әкеледі. Осыған байланысты M2M құрылғыларының, бағдарламалық жасақтаманың және берілетін деректердің тұтастығын тексеру, соның ішінде сәйкестендіру модульдерінің түпнұсқалығын тексеру қажет.

- M2M құрылғыларының өкілеттіктерін өзгерту парольдер мен кіру кілттерін таңдау, үшінші тарап арналары арқылы шабуыл жасау және MCIM сәйкестендіру модульдерін клондау болып табылады.

- Конфигурацияға әсер ету: бағдарламалық жасақтаманы жалған жаңарту және M2M құрылғыларының конфигурациясын өзгерту, пайдаланушы параметрлерін және кіруді басқару параметрлерін өзгерту.

- Құрылғыға желілік шабуылдар: M2M құрылғыларының функционалдығына және желілік протоколдардың әлсіз жақтарын қолдана отырып, олар жіберетін мәліметтерге әсер ететін "ортадағы адам" шабуылдары және DoS шабуылдары.

- Базалық желіге әсер ету ұялы байланыс операторы үшін негізгі қауіп болып табылады. Оларға: құрылғыларды заңсыз қосу, желіаралық экрандарды айналып өту үшін трафикті туннельдеу, базалық желіге DoS - шабуылдар, құрылғылардың рұқсат етілген орнын өзгерту, сондай-ақ алаяқтық құрылғыларды пайдалана отырып, радиоға қол жеткізу желісіне шабуылдар жатады.

- Құпия пайдаланушы деректеріне шабуыл жасау: деректерді беру желісі бойынша берілетін ақпараттық деректерді тыңдау, басқа пайдаланушылар түріндегі М2М желісіне қосылу, сондай-ақ құпия пайдаланушы деректерін уәкілетті емес үшінші тұлғаларға беру және т. б.

М2М желісінің жұмыс істеу қауіпсіздігін қамтамасыз ету, оның ішінде желінің қызмет көрсету сапасы мен қауіпсіздігін қамтамасыз ету, пайдаланушы деректерін беру және сақтау қауіпсіздігі М2М қызмет көрсету сервис-провайдерлерінің, қол жеткізу желілері операторларының, байланысты Стандарттау және реттеу органдарының басым міндеті болып табылады.

M2M желілерінің қауіпсіздігіне қойылатын талаптар. M2M желілері әсер ететін көптеген түрлі қауіпсіздік қатерлерін ескере отырып, M2M ETSI техникалық комитеті TS 102 689 техникалық сипаттамасында сипатталған осы желілер үшін қауіпсіздік талаптарын қалыптастырды. ETSI талаптарына сәйкес:

- M2M желісі M2M негізгі желісі мен M2M құрылғылары/шлюздері арасында бір жақты аутентификацияны қолдауы керек

M2M негізгі желісімен M2M құрылғыларын/шлюздерін аутентификациялау. әрбір M2M қосымшасы M2M шлюзі арқылы қосылған M2M құрылғылары үшін бірдей құрылғымен жұмыс істейтін басқа қосымшаларға тәуелсіз аутентификацияны орындай алуы керек. Аутентификация тікелей M2M базалық желісінде немесе M2M шлюзінде жүзеге асырылуы мүмкін, ол базалық желіде аутентификациядан өтті;

- M2M сыртқы қосымшасы тарапынан M2M құрылғысына/шлюзіне кіру сұранысы келіп түскен кезде, M2M тиісті құрылғысы/шлюзі кіруді сұраған M2M қосымшасымен өзара аутентификацияны инициализациялау мүмкіндігіне ие болуы керек;

- M2M желісі кейбір M2M қосымшалары мұндай құпиялылықты пайдалануды қажет етпеуі мүмкін болса да, желінің әртүрлі элементтері арасында мәліметтер алмасудың құпиялылығын сақтауы керек;

- M2M желісі қабылданған деректердің тұтастығын тексеруді қолдауы керек;

- М2М желісінің қауіпсіздігін қамтамасыз ететін шешімдер М2М құрылғыларын/шлюздерін рұқсатсыз пайдалануды болдырмауы тиіс;

- M2M желісі сақталған пайдаланушы деректеріне қол жеткізуді қамтамасыз етуі керек;

- егер бірнеше байланыс операторлары немесе сервис-провайдерлер М2М қызметін ұйымдастыруға және ұсынуға қатысқан жағдайда, M2M желісі қызметтің толассыз қауіпсіздігін қамтамасыз етуі тиіс;

- M2M желісі M2M құрылғыларының/шлюздерінің тұтастығын тексеру механизмін қолдауы керек, ал M2M құрылғысының/шлюзінің өзі мұндай тексеруді қолдамауы мүмкін. Егер М2М құрылғысы/шлюзі тұтастықты тексеруді қолдаса және тексеру сәтсіз болса, М2М құрылғысын/шлюзін одан әрі аутентификациялауға жол берілмейді.

M2M құрылғысының/шлюзінің тұтастығын тексеру M2M негізгі желісінен сұрау негізінде кез келген уақытта басталуы мүмкін немесе M2M құрылғысы/шлюзі жергілікті түрде іске қосылуы мүмкін.

Егер M2M құрылғысының тұтастығын тексеру қажет болса, бұл құрылғы құпия кілттер сияқты құпия ақпаратты сақтау және тексеру криптографиялық есептеулерді орындау үшін жеткілікті қорғалған аймаққа ие болуы керек. Тұтастықты тексеру барысында алынған барлық деректер рұқсат етілмеген сыртқы құрылғылар мен қосымшалар үшін қол жетімді болмауы керек.

M2M желілері, егер қауіпсіздік саясатымен рұқсат етілсе, бағдарламаларды жаңартуды, жаңа параметрлерді, құпия кілттерді және M2M құрылғыларында/шлюздерінде криптографиялық алгоритмдерді жою мүмкіндігіне ие болуы тиіс.

М2М желілерінің қауіпсіздігін қамтамасыз ету әдістері. Шифрлау және тұтастықты қорғау. M2M желісінде берілетін деректердің қауіпсіздігін қамтамасыз ету үшін әртүрлі криптографиялық операциялар қолданылады. Бұл ретте

ақпараттық хабарламаларды бақылау және деректердің тұтастығын қорғау оларды байланыс сессиясының қатысушыларына ғана белгілі құпия кілттің көмегімен хэштеу және ақпараттық хабарламаның соңында хэш-кодты беру арқылы жүзеге асырылады. Ақпараттық хабарламаны алушы бірдей құпия кілтті қолдана отырып, қабылданған деректердің хэш кодын есептеп, оны тарату жағында есептелген хэш кодымен салыстыра алады. Егер хэш кодтары сәйкес келсе, алушы хабарламаның түпнұсқалығына сенімді бола алады. Осылайша, M2M желісіндегі ақпаратты өзгерту шабуылдаушыға құпия кілт белгілі болған жағдайда ғана орынды болады. ETSI техникалық сипаттамаларында ұсынылған хэш алгоритмдерінің бірі-HMAC-SHA256 алгоритмі, ол 256 биттік хэш мәндерін жасайды.

Ақпараттық деректерді және басқару командаларын шифрлау желі арқылы берілетін құпия ақпаратты, M2M құрылғысының идентификаторларын тыңдаудан және ауыстырудан қорғауға мүмкіндік береді. Шифрлау үшін des (Data Encryption Standard) және AES (Advanced Encryption Standard) алгоритмдері қолданылады.

Көптеген криптографиялық операциялардың кемшіліктері-M2M арзан құрылғыларында болмауы мүмкін үлкен қажетті есептеу ресурстары. сонымен қатар, Пайдаланушы ақпаратының тұтастығын қорғау радио қол жетімділік желісі арқылы берілетін деректердің көбеюіне әкеледі. Іс жүзінде пайдаланушы ақпаратын шифрлау кеңінен қолданылады және басқару және сигнал беру командалары әдетте тұтастықты қорғау арқылы беріледі. Сигнал хабарламаларының саны шектеулі және олар кездейсоқ болғандықтан, осы хабарламалардың тұтастығын қорғауға байланысты үстеме шығындар желінің жұмысына аздап әсер етеді.

IP-адрестерге негізделген сүзу. Пайдаланушы құрылғыларын дербестендіру және желілік шабуылдардың алдын алу үшін аралық маршрутизаторлардағы пакет көздерінің IP-мекенжайларын олардың жүру жолы бойында тексеру жүргізіледі. Мұндай тексеру кіріс пакеттерін маршруттау кестелері арқылы тексеруді және бастапқы IP мекен-жайына кері жолды іздеуді, IPCP немесе DHCP протоколдарын қолдана отырып, IP мекенжайы мен құрылғының MAC мекен-жайын салыстыруды қамтиды [4]. Алайда, қауіпсіздікті тексерудің мұндай әдістері жеткіліксіз, өйткені:

- қауіпсіздікке қауіп төндіретін құрылғы шабуылға ұшыраған құрылғыға тікелей желіде орналасуы мүмкін;

-тіркеу процедурасы кезінде хабарлама көзінің заңды IP-мекен-жайы (уақытша немесе тұрақты) тыңдалуы мүмкін;

- радиоқолжетімділік желісінің схемасына байланысты абоненттік құрылғылардан шығатын пакеттерде қандай да бір құрылғы сәйкестендіргіштері болмауы мүмкін.

Пакет көздерінің IP мекенжайлары туралы ақпаратты пайдаланатын M2M желілерінің қауіпсіздігін қамтамасыз етудің басқа әдістері мониторинг болып табылады

трафикті жіктеу. Бұл әдістердің негізгі мақсаты қауіп-қатерге ұшыраған клиенттік құрылғыларды бақылау есебінен желілік ауытқуларды анықтау болып табылады. Мысалы, оның көлемінің трафик құрылымының өзгеруін, сондай-ақ бұрын алмасу болмаған жаңа соңғы құрылғылармен деректер алмасуды анықтау. Мұндай механизмдер негізінен "желілік құрттарды" анықтау үшін қолданылады, бірақ олар ұрланған M2M құрылғыларын анықтау үшін тиімсіз, өйткені шабуылдаушы көптеген заңды IP мекенжайларын және желілік сниферлермен ұсталған уақытша идентификаторларды қолдана отырып деректерді жібере алады. Сонымен қатар, трафик мониторы / классификаторы зиянды трафикті тиімді анықтай алмайды, өйткені ол көптеген заңды жіберушілер арасында біркелкі бөлінеді.