ҚАЗАҚСТАН РЕСПУБЛИКАСЫ ҒЫЛЫМ ЖӘНЕ ЖОҒАРЫ БІЛІМ МИНИСТРЛІГІ

«Л.Н. ГУМИЛЕВ АТЫНДАҒЫ ЕУРАЗИЯ ҰЛТТЫҚ УНИВЕРСИТЕТІ» КЕАҚ

Студенттер мен жас ғалымдардың
«ǴYLYM JÁNE BILIM - 2024»
XIX Халықаралық ғылыми конференциясының
БАЯНДАМАЛАР ЖИНАҒЫ

СБОРНИК МАТЕРИАЛОВ
XIX Международной научной конференции
студентов и молодых ученых
«ǴYLYM JÁNE BILIM - 2024»

PROCEEDINGS
of the XIX International Scientific Conference
for students and young scholars
«ǴYLYM JÁNE BILIM - 2024»

2024
Астана

УДК 001
ББК 72
G99

«ǴYLYM JÁNE BILIM – 2024» студенттер мен жас ғалымдардың XIX Халықаралық ғылыми конференциясы = XIX Международная научная конференция студентов и молодых ученых «ǴYLYM JÁNE BILIM – 2024» = The XIX International Scientific Conference for students and young scholars «ǴYLYM JÁNE BILIM – 2024». – Астана: – 7478 б. - қазақша, орысша, ағылшынша.

ISBN 978-601-7697-07-5

Жинаққа студенттердің, магистранттардың, докоранттардың және жас ғалымдардың жаратылыстану-техникалық және гуманитарлық ғылымдардың өзекті мәселелері бойынша баяндамалары енгізілген.

The proceedings are the papers of students, undergraduates, doctoral students and young researchers on topical issues of natural and technical sciences and humanities.

В сборник вошли доклады студентов, магистрантов, докторантов имолодых ученых по актуальным вопросам естественно-технических и гуманитарных наук.

УДК 001
ББК 72
G99

ISBN 978-601-7697-07-5

УДК 004.056

ЗАТТАР ИНТЕРНЕТІНІҢ ОСАЛДЫҚТАРЫН ТАЛДАУ ЖӘНЕ ОЛАРДЫ ЖОЮДЫҢ СТРАТЕГИЯЛЫҚ ТӘСІЛДЕРІ

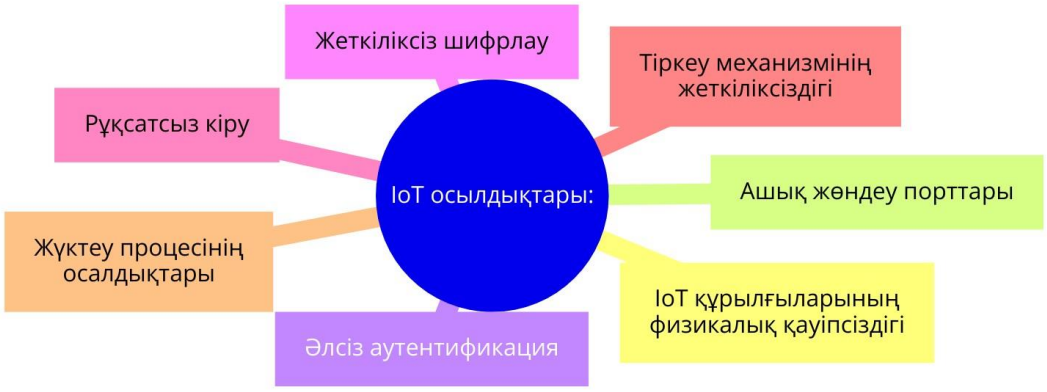
Қаныбек Таңшолпан Шәмшидинқызы
mereke.kanybek@mail.ru
Л.Н. Гумилев атындағы ЕҰУ Ақпараттық қауіпсіздік мамандығының
1 курс магистранты, Астана, Қазақстан
Ғылыми жетекшісі – А.С. Баегизова

Аннотация: Бұл мақалада заттар интернеті (IoT) технологияларының кең таралуынан туындайтын маңызды қауіпсіздік мәселелері қарастырылады. Қазіргі уақытта заттар интернеті байланыс жүйесінде маңызды рөл атқарады, ақылды қалалар, ақылды үйлер, ақылды көлік және т.б. IoT құрылғылары күн сайын жаңа шабуылдарға ұшырайды, бұл дәстүрлі қауіпсіздік шешімдері жеткіліксіз болуы мүмкін өзара байланысты IoT құрылғыларының айқын осалдықтарын көрсетеді. Мақаланың мақсаты - заттар интернеті жүйелеріндегі осалдықтарды анықтау, тәуекелдерді азайту және қауіпсіздігін арттыруға мүмкіндік беретін жою стратегияларын ұсыну. Мақалада заттар интернетіне қатысты қауіпсіздік мәселелері қарастырылады және болашақта қауіпсіздікті нығайту үшін ұсынылатын стратегиялар талданады.

Кілтті сөздер: Заттар интернеті IoT, аутентификаци, шифрлау, заттар интернетінің қауіпсіздігі (IoT).

Жаһандық цифрландыру жаңа ақпараттық технологиялардың пайда болуымен және тұтынушылық артықшылықтардың өзгеруімен жеделдеді. Қазіргі уақытта әлемде миллиардтан астам қосылған құрылғылар бар және бұл сан жыл сайын өсуде. 2025 жылға қарай заттар интернетіне (IoT) қосылған 75 миллиардтан астам құрылғы пайдаланылады деп болжануда [1]. Заттар интернеті (IoT) сенсорлар, интернетке қосылған жетектер сияқты жердегі құрылғылар жинайтын деректерді түсіну арқылы қоршаған ортаны қашықтан басқаруға және бақылауға мүмкіндік береді. Жалпы, интеллектуалды қызметтерді пайдалану үшін осал құрылғыларды интернетке қосатынымыз анықталды [2]. IoT құрылғылары нарыққа операциялық жүйенің ескірген нұсқалары, жаңарту механизмдерінің жоқтығы, әдепкі құпия сөздер және ашық порттар сияқты белгілі осалдықтармен шығуда [3]. Mirai, Brickerbot және Hijame сияқты ботнеттер бұл саңылауларды бірнеше сағат бойы әртүрлі қызметтерді өшіретін боттардың армиясын құру үшін пайдаланады [4]. Сонымен қатар, хакерлер радио бақылаушылар мен бейне бақылаушы ойыншықтар, ата-аналар мен олардың балаларының миллиондаған дауыстық жазбалары, тіркелгілер, құпия сөздер және т.б. алу үшін пайдаланды. Шабуыл жасаушылар тіпті IoT құрылғыларының микробағдарламасын оңай қайта бағдарламалай алады. Сондықтан, бұл мақалада біз ең алдымен ықтимал қарсыластар пайдаланатын IoT құрылғыларындағы негізгі осалдықтарға назар аударды қ. Бұған қоса, біз осы осалдылықтардан қорғау үшін қабылдауға болатын жеңілдету стратегияларын ұсынамыз.

Заттар интернетінің қауіпсіздігі қазіргі кездегі өзекті мәселе болып табылады. Қауіпті шабуылдарды іске қосу үшін қауіпсіздік саңылаулары, атап айтқанда IoT жүйелеріндегі осалдықтар және оларды орналастыру конфигурациялары пайдаланылады. Заттар интернетінің өзінің керемет мүмкіндіктерін жоғалту алдында тұр. Мұндай жағдайда осалдықты бағалау IoT құрылғыларын осы пайда болатын қауіптерден қорғауды бастау үшін бірінші орын болуы керек [5]. 1-ші суретте көрсетілгендей, IoT-те жиі кездесетін осалдықтарды анықтау және оларға тиімді жауап қайтару стратегияларын құру зор маңызға ие.



Сурет 1. IoT-те жиі кездесетін осалдықтар

– IoT құрылғыларының физикалық қауіпсіздігі. Техникалық қызмет көрсетілмейтін ортадағы IoT құрылғыларының көпшілігі қуат тұтыну және өңдеу уақыты сияқты жанама арналар арқылы ақпарат алу үшін пайдаланылуы мүмкін. Шабуылдаушы сонымен қатар бірнеше шабуылдарды бастау үшін пайдаланылуы мүмкін заттар интернетінің түйіндерінің клондарын жасай алады. Олар сондай-ақ осы бұзылған түйіндердің тіркелгі деректеріне оңай қол жеткізе алады [6].

– Ашық жөндеу порттары. IoT жүйесін реттеу үшін барлық мүмкін тәсілдермен пайдаланылады. Осы осал порттардан шабуылдаушы зиянды кодты енгізу, кірістірілген бағдарламалық құралды жалған өзгерту және олардың қорғанысын айналып өту сияқты шабуылдарды бастауы мүмкін. Mirai, Hajime, Bricker сияқты ботнеттер "қызмет көрсетуден бас тарту" сияқты әртүрлі шабуыл опцияларын іске қосу үшін telnet портын пайдаланды".

– Әлсіз аутентификация. Бұл ресурстары шектеулі заттар интернеті түйіндерінде сенімді аутентификация механизмдерін енгізуде көптеген қиындықтар туғызды. Ақылды субъектілер IoT жүйесіне оңай еніп, жеке басын тексеруден аулақ болады, осылайша жүйені көптеген жолдармен қолданады. Осы осалдықты пайдаланып ұйымдастырылған шабуылдардың кейбіріне DDoS шабуылы, сөздік шабуылы, Sybil шабуылы, Hello flood және үйге шабуыл кіреді [7].

– Жеткіліксіз шифрлау. Сымсыз байланыс деректердің бұзылуы және құпиялылық тұрғысынан көбірек қиындықтар туғызады. Барлық дерлік интернет құрылғылары сымсыз медианы пайдаланатыны анықталды. Сенімсіз медиа бола отырып, пайдаланушының жеке ақпараты жалған ақпарат беру шабуылдарына көбірек ұшырайды. Сенімді шифрлау механизмі деректердің ағып кетуіне жол бермейді. Дегенмен, сенімді криптографиялық алгоритмді енгізу ресурс шектеулі IoT құрылғылары үшін күрделі тапсырмаға айналады. Бұл сақтау шабуылдары, тыңдау және "ортадағы адам" шабуылы сияқты шабуылдарға әкелуі мүмкін [8].

– Рұқсатсыз кіру. IoT жүйелері мен деректеріне рұқсатсыз кіру тек уәкілетті ұйымдарға қолжетімді болуы керек. Ол үшін сенімді тіркелгі деректері жүйесін енгізу керек. IoT құрылғылары құпия сөздердің жеткілікті күрделілігін қамтамасыз етпейтіні анықталды. Тіпті кейбір құрылғылар әдепкі құпия сөздерді қолдана береді және осылайша зиянкестердің тұзағына түседі. Өндірушілер қатты кодталған құпия сөздері бар құрылғыларды жеткізу арқылы қондырманы қамтамасыз етеді. Демек, оңай рұқсатсыз кіру бүкіл заттар интернеті жүйесінің деректері мен қауіпсіздігіне қауіп төндіреді.

– Тіркеу механизмінің жеткіліксіздігі. Тіркеудің дұрыс механизмімен біз шабуылдар мен бұзу әрекеттерін анықтай аламыз. Әкімшілер сәтті және сәтсіз аутентификация әрекеттеріне, кіру әрекеттеріне және авторизация әрекеттеріне қатысты оқиғаларды тіркеуі керек. Заңсыз пайдалануды болдырмау үшін журналдың барлық ақпараты шифрланған түрде сақталуы керек.

– Жүктеу процесінің осалдықтары. Жүктеу процесінің осалдықтарын қолдана отырып, шабуылдаушы бүкіл жүйені басқара алады. Ол кіру үшін жүктеу ретін, микробағдарламаны және жүктеушіні қолдана алады. Эксперименттік жағдайларда фитнес-трекер мен Nest термостатының жүктеу процесінің осалдықтарын пайдалану үшін шабуыл жасалды.

Бұл бөлімде осы өсіп келе жатқан осалдықтарды жою үшін қабылдануы мүмкін кейбір түзету стратегиялары талқыланады [9]. 2-ші суретте көрсетілгендей IoT құрылғыларының қауіпсіздігін нығайту және осал тұстарын болдырмау үшін қабылданатын шаралардың кең спектрін көрсетеді.

Сурет 2. IoT қауіпсіздігін жою стратегиялары

– Бүйірлік арналарды талдау. Біз бүйірлік арна сигналын талдау арқылы құрылғыдағы зиянды микробағдарлама мен аппараттық трояндарды анықтай аламыз. Трояндарды анықтау үшін қуат тұтыну, синхрондау сигналдары, кеңістіктік талаптар және температура сияқты сигналдар қолданылады. Дәл осылай троян әсер еткен микросұлбамен және трояндары жоқ микросұлбамен салыстыруға болады. Уақытқа негізделген схемалар кідірту сынақтары арқылы трояндарды анықтайды, қуатқа негізделген схемалар белсенді бақылауды пайдаланады және әлеуметтік температураға негізделген схемалар инфрақызыл бейнелеу механизмдерін пайдаланады. Сол сияқты, бүйірлік арналар туралы ақпаратты жүйеде зиянды микробағдарламаның болуын білдіретін машинаның қалыптан тыс әрекетін анықтау үшін пайдалануға болады.

– Саясатқа негізделген механизмдер және шабуылды анықтау жүйелері. IoT ортасында енуді анықтау жүйелерін енгізу арқылы біз өзімізді қауіпсіздік пен құпиялылық мәселелерінен айтарлықтай қорғай аламыз. Бұл анықтау жүйелері кез келген маңызды саясаттардың бұзылғанын анықтай алады және осылайша кірулерді анықтай алады. Бұған қоса, бұл жүйелер IoT түйініне әдеттен тыс сұрауларды тану арқылы ұйқының жетіспеушілігінен және батареяның таусылуына шабуылдарынан қорғауда пайдалы екені дәлелденді.

– Схеманы модификациялау. Физикалық шабуылдар, трояндық шабуылдар және бүйірлік арналардағы шабуылдарды схеманы өзгерту арқылы да қорғауға болады. IoT түйіндерінің физикалық жабдықтарындағы интеграцияланған қауіпсіздік механизмі осы шабуылдардан физикалық қорғанысты арттырады. Мысалы, түтін детекторлары сияқты үйді

автоматтандыру датчиктері көптеген механикалық/электрлік рұқсатсыз қорғаныс құралдарын пайдаланады. Сол сияқты, бүйірлік арна ақпараты схеманы өзгерту арқылы бұрмаланған ақпаратты беру арқылы зиянкестерден де қорғалуы мүмкін. Кейбір танымал тәсілдер рандомизацияланған кідірісті, шуды, хамминг салмағын және кэш архитектурасын өзгертуді қолданады. Сонымен қатар, PUF-ті схемаға біріктіру арқылы біз аутентификацияны, трояндық бағдарламаларды анықтауды және құрылғыны сәйкестендіруді қоса аламыз. PUF-бұл физикалық қол жетімсіз, рұқсатсыз кіруден қорғалған және болжау мүмкін емес чипке салынған физикалық қол жетімсіз функция.

– Кірістірілген бағдарламалық жасақтаманы жаңарту қауіпсіздігін қамтамасыз ету. Қауіпсіз бағдарламалық жасақтаманы жаңарту кірістірілген бағдарламалық жасақтаманы қашықтан немесе тікелей жаңартудың екі әдісі бар. Бірінші жағдайда, сервер кірістірілген бағдарламалық жасақтаманың жаңа нұсқасының қол жетімділігі туралы хабарлайтын сигналды (CMD) жібереді. Содан кейін кірістірілген бағдарламалық жасақтаманың жаңартылған нұсқасы бар түйін жарнаманы (ADV) көрші түйіндеріне жібереді. ADV хабарламасы бар дауыссыз түйіндер ендірілген бағдарламалық жасақтаманың жаңа нұсқасын бар бағдарламамен салыстырады. Егер олар жаңартуды қажет етсе, олар сұрау жібереді (REQ) және осылайша жаңарту файлын алады. Кірістірілген бағдарламалық жасақтаманы қауіпсіз қашықтан жаңарту үшін барлық CMD, ADD, REQ және data пакеттері аутентификациялануы керек. Кірістірілген бағдарламалық жасақтаманы тікелей жаңарту кезінде, мысалы, USB кабелі арқылы, кірістірілген бағдарламалық жасақтаманың тұтастығын және пайдаланушының аутентификациясын ескеру қажет. Бұл талапты орындамау шабуылдаушыға құрылғының заңды микробағдарламасының орнына зиянды бағдарламаны орнатуға мүмкіндік береді.

– Криптографиялық схемалар. Байланыс деңгейінде біз ұстап алу және маршруттау сияқты шабуылдардан қорғау механизмі ретінде сенімді шифрлау сияқты криптографиялық схемаларды пайдалана аламыз. Ескі криптографиялық әдістерді ресурстары шектеулі IoT түйіндерінде бұл мәселелерді шешу үшін пайдалану мүмкін болмады. Бұл әдістер жадты пайдалануды, қуат тұтынуды, пакеттердің жоғалуын және кідірісті арттырады. IoT жүйесінде PRESENT және CLEFIA сияқты байланыстарды қорғау үшін жеңіл криптографиялық әдістерді әзірлеуге көп күш жұмсалды. Дегенмен, құпиялылықты қамтамасыз ете отырып, жеңіл IoT талаптарын қанағаттандыру үшін ашық кілттерді шифрлау әдістерінің жетіспеушілігі бар.

– Депаттернизация және орталықсыздандыру. Анонимділіктен және бүйірлік арналардағы шабуылдардан қорғаудың тағы бір механизмі-депаттернизация және орталықсыздандыру. Жалған пакеттер арқылы деректер трафигінің құрылымын өзгерту арқылы біз бүйірлік арналардағы шабуылдардан қорғай аламыз. Сонымен қатар, орталықсыздандыру құпия деректерді байланыстырушы ағаш арқылы таратын анонимділікті қамтамасыз етеді, сондықтан ешқандай түйін бастапқы деректердің толық бейнесін ала алмайды.

– Бағдарламалық жасақтама кепілдігі. Бағдарламалық жасақтама кепілдігі бағдарламалық жасақтама жүйелерінің қауіпсіздігі мен сенімділігін қамтамасыз етуде маңызды рөл атқарады, бұл IoT құрылғыларының кең таралуын ескере отырып өте маңызды. Бұл процесс жобалаудың бастапқы кезеңінен бастап орналастыру мен қызмет көрсетуге дейінгі осалдықтарды анықтау және жою стратегияларын қамтиды. Бағдарламалық жасақтаманың тиімді кепілдігі қауіпсіздікті бағдарламалық жасақтаманы әзірлеудің өмірлік цикліне біріктіруді, бағдарламалық жасақтаманың жаңартуларының тұтастығын қамтамасыз етуді, түзетулерді мұқият басқаруды, сенімді криптографиялық әдістерді қолдануды және мүдделі тараптарды қауіпсіздіктің озық тәжірибелеріне үйретуді қамтиды. Бағдарламалық жасақтама кепілдігінің мақсаты - шабуылға төзімді және сыртқы қауіптерге тап болған кезде де қауіпсіз және сенімді жұмыс істейтін бағдарламалық жасақтаманы құру.

– Қауіпсіздік хаттамалары. Заттар интернетінің ресурстарының шектеулі болуы оларды барған сайын осал етеді, өйткені оларда шектеулі қауіпсіздік механизмдері болуы

мүмкін. Осы мақсатта энергия тұтынуды ескеретін IoT экожүйелерін дамытуға күш салынуда. Осындай архитектуралардың бірі, яғни 2EA архитектурасы balasubramanian et al әзірлеген. Energyaware-Edge-Aware (2EA) архитектурасында IoT сенсорлары өз энергиясын жинай алады. Заттар интернеті желісіндегі әрбір сенсор үшін қуат көрсеткіштері бар энергетикалық профиль сақталады. Энергия таусылған жағдайда, зардап шеккен түйін энергия профилін сұрайды және жақын жерде ең сенімді түйінді табады. Бұл схема тапсырмаларды қабылдау процесіне негізделген ресурстарды оңтайлы пайдалануды қамтамасыз етеді.

Бұл мақалада заттар интернетінің (IoT) өсіп келе жатқан осалдықтары жан-жақты зерттелді және оларды жоюдың түрлі стратегиялары ұсынылды. IoT құрылғыларының күнделікті өмірімізде алатын орны артып келе жатқанына қарамастан, олардың қауіпсіздігі әлі де негізгі алаңдаушылық тудырады. Мақалада талқыланған осалдықтар мен түзету стратегиялары IoT қауіпсіздігін нығайтуға және потенциалды шабуылдарға тиімді жауап беруге бағытталған. IoT құрылғыларын тиімді қорғау үшін үздіксіз зерттеулер мен әзірлемелерді жалғастыру қажеттігі айқын көрінеді. Болашақта IoT қауіпсіздігі саласындағы зерттеулер мен әзірлемелер бұл технологияның әлеуетін толық пайдалануға және кибер қауіптерге қарсы тұра алатын сенімді шешімдер құруға ықпал етуі тиіс.

Қолданылған әдебиеттер тізімі

1. Zanella A. et al. Internet of things for smart cities //IEEE Internet of Things journal. – 2014. – Т. 1. – №. 1. – С. 22-32.

2. Mikko H. et al. The internet of (vulnerable) things: On hypponen's law, security engineering, and IoT legislation//Technology Innovation Management Review. – 2017.

3. Corser G., Fink G., Bielby J. Internet of Things (IoT) Security Best Practices; IEEE Internet Technology Policy Community; White Paper//IEEE: Piscataway, NJ, USA. – 2017.

4. Kolias C. et al. DDoS in the IoT: Mirai and other botnets//Computer. – 2017. – Т. 50. – №. 7. – С. 80-84.

5. Anand P. et al. IoT vulnerability assessment for sustainable computing: threats, current solutions, and open challenges//IEEE Access. – 2020. – Т. 8. – С. 168825-168853.

6. Makhdoom I. et al. Anatomy of threats to the internet of things //IEEE communications surveys & tutorials. – 2018. – Т. 21. – №. 2. – С. 1636-1675.

7. Rajan A., Jithish J., Sankaran S. Sybil attack in IOT: Modelling and defenses//2017 International conference on advances in computing, communications and informatics (ICACCI). – IEEE, 2017. – С. 2323-2327.

8. Neshenko N. et al. Demystifying IoT security: An exhaustive survey on IoT vulnerabilities and a first empirical look on Internet-scale IoT exploitations//IEEE Communications Surveys & Tutorials. – 2019. – Т. 21. – №. 3. – С. 2702-2733.

9. Mosenia A., Jha N. K. A comprehensive study of security of internet-of-things//IEEE Transactions on emerging topics in computing. – 2016. – Т. 5. – №. 4. – С. 586-602.

ӘОЖ 004.056.57

PORTABLE EXECUTABLE ФОРМАТТЫ ФАЙЛДАР ҚҰРЫЛЫМЫ ЖӘНЕ ОЛАРДЫ ЗИЯНДЫ КОДҚА АЙНАЛДЫРУ ЖОЛДАРЫ

Мукушев Әмірбек Қайратұлы

Amirbek.mukushef@gmail.com

Л.Н.Гумилев атындағы ЕҰУ Ақпараттық технологиялар факультетінің Ақпараттық қауіпсіздік кафедрасы магистранты , Астана, Қазақстан

Ғылыми жетекші – Суханова Ж.С.

Аннотация. Windows операциялық жүйесі қолданушылар арасында кең таралған жүйе. Windows жүйесіндегі барлық орындалатын файлдар Portable Executable форматына сәйкес құрастырылады. Оның ішінде зиянды программалар да Portable Executable форматына ие.