$$K_{\min} > L + p \quad (4)$$

L-ді төрт секторға (4 * 4208) тең деп, р төртке тең болса, $K_{\min} > 16836$ бит > 4 секторды аламыз. Осылайша, кодтар тобының артық бөлігі сынақ бөлігінің ұзындығының көптігін, сектор көлемін ескере отырып, кем дегенде 5 сектордан тұруы керек.

Айта кету керек, әр түрлі конфигурациялардың қателіктерінің теориялық есептеулері АССЖ тестілері кезінде алынған тәжірибелік мәліметтермен толық расталған. Дискпен жұмыс жасау деңгейіндегі қателіктер туралы статистикалық мәліметтерді жинау үшін бағдарламалар пакеті іске асырылды, қабылдау тесттері аясында іргелес бірнеше секторда сәтсіздіктердің пайда болуы бірнеше рет тіркелді.

Қолданылған әдебиеттер тізімі

1. Арбо-Соренсен Р. Сбои полупроводниковых запоминающих устройств при полетах спутников. // Москва: ВИНИТИ Надёжность и контроль качества №27. 2013.-С.25-28.
2. Алексеев В.Б., Сложность умножения матриц. // Кибернетический сборник. М: Мир, 2019. - №25 - С.72-89.
3. Амербаев В.М. под ред. Теория кодирования и оптимизация сложных систем. // М.: Наука, 2017. - 217с.
4. Ахо А., Хопкрофт Дж. Построение и анализ вычислительных алгоритмов. //М.: Мир, 2016.-420 с.
5. Ахо А.В., Хопкрофт Д. Э., Ульман Д.Д. Структуры данных и алгоритмы. // М.: Вильяме, 2018.-356 с.

ОӘЖ 003.26.09

ТӨМЕН РЕСУРСТЫ КРИПТОГРАФИЯ ӘДІСТЕРІН ҚОЛ ЖЕТІМДІ БАҚЫЛАУ ЖӘНЕ БАСҚАРУ ЖҮЙЕСІНДЕ ҚОЛДАНУ

Әбілбек Ақниет Мықтыбекқызы

akniet.abilbek@mail.ru

Л.Н.Гумилев атындағы Еуразия ұлттық университеті 7М06103 магистранты

Нұр-Сұлтан қ, Қазақстан

Ғылыми жетекішісі - А.А.Муханова

Л.Н.Гумилев атындағы Еуразия ұлттық университетінің ақпараттық жүйелер кафедрасының аға оқытушысы Оспанов Руслан Маратович

Нұр-Сұлтан қ, Қазақстан

Біздің дәстүрлі криптография әдістері, мысалы, AES (шифрлау), SHA-256 (хэширлеу) және RSA/эллиптикалық қисық (қолы) сияқты, ақылға қонымды есептеу қуаты мен жад мүмкіндігі бар жүйелерде жақсы жұмыс істейді, олар ендірілген жүйелер мен сенсорлық желілер бар әлемде нашар масштабталады. Осылайша, қарапайым криптографияның көптеген мәселелерін шешу үшін криптографияның оңай әдістері ұсынылады. Бұл физикалық өлшеммен, өңдеу талаптарымен, жадының шектелуімен және энергия шығынымен байланысты шектеулерді қамтиды.

AES және SHA компьютерлік жүйелерде жақсы жұмыс істейді. Дегенмен, ресурстары шектеулі құрылғылар үшін көптеген жеңіл криптографиялық примитивтер ұсынылды және қолданылды. Ұлттық (NIST) және халықаралық (ISO / IEC) ұйымдар жеңілдетілген криптография үшін қолдануға болатын және Internet of Things (IoT) және radio frequency identification (RFID) құрылғыларында пайдалы болуы мүмкін бірқатар әдістерді сипаттайды [1]. Олар құрылғы спектрін келесідей анықтайды:

- Әдеттегі криптография. Серверлер мен десктоптар; планшеттер мен смартфондар.
- Жеңіл криптография. Орнатылған жүйелер; RFID және сенсорлық желілер.

IoT құрылғыларының көпшілігі көп пайдалы режимде жұмыс істейтіндіктен, бағдарламалық қамтамасыз ету өнімділігі жеңіл криптография үшін шешуші мәнге ие және Chaskey, FLY, LEA, SPARX және т.б. сияқты қолданыстағы жеңіл шешімдер жақсы бағалау нәтижелерін көрсетеді. IoT жағдайында шифрлардың түрлерін, блоктың өлшемін, кілттің өлшемін, тиісті шабуылдарды және т. б. ескеріңіз. Криптоанализде әдеттегі шабуылдар бір кілтті / байланысты кілтті пайдалануды, кілтті ажыратуды / қалпына келтіруді, әлсіз кілттерді, делдалды пайдаланып шабуылдарды және т.б. қамтиды [2].

Сонымен қатар, әртүрлі байланыс технологияларын қолдану арқылы аппараттық деңгейде де, бағдарламалық деңгейде де іске асырылуы мүмкін, IOT соңғы түйіндері мен RFID белгілері сияқты ресурстары шектеулі құрылғылардың өте кең ауқымына арналған. Ресурстары шектеулі ортада стандартты криптографиялық алгоритмдерді іске асыру көлеміне, жылдамдығына немесе өткізу қабілетіне және энергия тұтынуына байланысты іске асыру өте қиын. Жеңілдетілген криптография ресурстары шектеулі құрылғыларда енгізу құнын, жылдамдығын, қауіпсіздігін, өнімділігін және энергияны тұтынуды төмендетеді. Жеңілдетілген криптографияны ынталандыру аз жадты, аз есептеу ресурстарын және аз энергияны шектеулі ресурстармен жұмыс істей алатын қауіпсіздікті қамтамасыз ету үшін пайдалану болып табылады. Жеңілдетілген криптография әдеттегі криптографиямен салыстырғанда оңай және жылдам күтіледі.

Төмен ресурсты криптография әдістері

PHOTON жеңіл криптографиясы үшін, SPONGENT және Lesamanta-LW ISO / IEC 29192-5: 2016, ISO / IEC 29192-2 : 2012 және ENOCORO және Trivium ISO / IEC 29192-3: 2012 шеңберінде блоктық әдістер үшін PRESENT және CLEFIA хештеу әдістеріне арналған стандарттар ретінде анықталған. Заманауи хэш-әдістердің көпшілігі IoT құрылғылары үшін тиімсіз [3]. Осылайша, NIST SPONGENT, PHOTON, Quark және Lesamnta-LW сияқты араластырудың жаңа әдістерін ұсынды.

Төмен ресурсты криптография әдістерін бақылау және басқару жүйесінде қолдану аса тиімді болып саналады.

Кез келген объектіні қорғау бірнеше шектерді қамтиды, олардың саны объектінің режимдік деңгейіне байланысты. Бұл ретте барлық жағдайларда объектіге кіруді қол жетімді бақылауды басқару жүйесі маңызды шетелде болады. Заманауи техникалық құралдарды пайдалану арқылы жақсы ұйымдастырылған қол жетімді бақылауды басқару жүйесі бірқатар міндеттерді шешуге мүмкіндік береді. Ең маңыздысы қатарына мыналарды жатқызуға болады: өнеркәсіптік шпионажға қарсы іс-қимыл; ұрлыққа қарсы іс-қимыл; материалдық құндылықтарды қасақана зақымдауға қарсы іс-қимыл; жұмыс уақытын есепке алу; қызметкерлердің келуі мен кетуінің уақтылығын бақылау; ақпараттың құпиялылығын қорғау; келушілер ағынын реттеу; көліктің кіруін және кетуін бақылау. Нақты қол жетімді бақылауды басқару жүйесі жүзеге асыру кезінде жеке тұлғаны сәйкестендіру және аутентификациялау үшін әртүрлі әдістер мен оларды іске асыратын құрылғыларды пайдаланады. қол жетімді бақылауды басқару жүйесі Ресейде де, шетелде де қауіпсіздік нарығының ең дамыған сегменттерінің бірі болып табылатынын атап өткен жөн. Бірқатар сарапшылардың деректері бойынша қол жетімді бақылауды басқару жүйесі нарығының жыл сайынғы өсімі 25% - дан астамды құрайды. Техникалық қауіпсіздік жүйесі саласында жұмыс істейтін мамандар саны 500 мың адамнан асты. Ең жиі қолданылатын қол жетімді бақылауды басқару жүйесі ретінде мыналар атауға болады:

— кәдімгі және қабырғалық турникеттер;
— дәліздерде өтуге арналған турникеттер;
— шлюздік кабиналар;
— автоматты калиткалар;
— роторлы турникеттер;
— айналмалы есіктер;
— жол блокираторлары;

— шлагбаумдар;
— тұрақ жүйелері;
— дөңгелек жылжымалы есіктер;
— үштангтық турникеттер;
— толық көлемді турникеттер;
— жылжымалы турникеттер.

Ашық хаттаманы пайдалана отырып, кез келген қауіпсіздік жүйесімен қол жетімді бақылауды басқару жүйесін интеграциялау мүмкіндігі туралы мәселе өте маңызды болып табылады [4].

Қолданыстағы (ГОСТ) МЕМСТ Р 51241-98 «кіруді бақылау және басқару құралдары мен жүйелері», ол жіктеуді, жалпы техникалық талаптарды және сынау әдістерін белгілейді, қол жетімді бақылау дәне басқару жүйесіне бөледі:

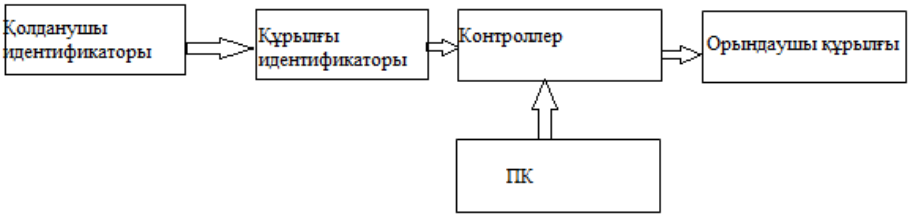
— басқару тәсілі бойынша;
— қол жеткізудің бақыланатын нүктелерінің саны;
— функционалдық сипаттамалары;
— бақылау объектілерінің түрі;
— жүйенің рұқсатсыз кіруден қорғалу деңгейі [5].

Р 78.36.005-99 құжатына сәйкес барлық қол жетімді бақылауды басқару жүйесі төрт классқа бөлінеді.

1-классты қол жетімді бақылауды басқару жүйесі – автономды режимде жұмыс істейтін және тиісті сәйкестендіргіші бар барлық тұлғаларға рұқсат беруді жүзеге асыратын аз функциялы жүйе. Мұндай жүйеде атқарушы құрылғыларды қолмен немесе автоматты басқару, сондай-ақ жарықтық немесе/және дыбыстық сигнал беру пайдаланылады.

2-ші класты қол жетімді бақылауды басқару жүйесі -монофункционалды жүйелер. Олар бір деңгейлі және көп деңгейлі болуы мүмкін және автономды және желілік режимдерде жұмысты қамтамасыз етеді. Адамдарды (адамдар топтарын) жіберу күні, уақытша интервалдар бойынша жүзеге асырылуы мүмкін. Жүйе оқиғалардың Автоматты тіркеуін және атқарушы құрылғыларды автоматты басқаруды қамтамасыз етуге қабілетті.

3-ші және 4-ші класстардың қол жетімді бақылауды басқару жүйесі әдетте желілік болып табылады. Онда аса күрделі идентификаторлар және желілік өзара әрекеттесудің әртүрлі деңгейлері (клиент-сервер, Виганда карталарын немесе магниттік карталарды оқитын интерфейстер, мамандандырылған интерфейстер және т.б.) қолданылады. Бүгінгі күні әртүрлі өндірушілердің қол жетімді бақылауды басқару жүйе түрлері, сондай-ақ оның компоненттері өте көп. Әрбір нақты кіру бақылау жүйесінің бірегейлігіне қарамастан, ол 4 негізгі элементтен тұрады: пайдаланушының идентификаторы (карта-пропуск, кілт), сәйкестендіру құрылғысы, басқарушы контроллер және атқарушы құрылғылар. Жалпы сызба сурет 1. көрсетілген.



Сурет 1. Қол жетімді бақылауды басқару жүйесінің жалпы сызбасы

Қол жетімділікті бақылау және басқару жүйесінің жұмысын оңайлатылған түрде келесі түрде сипаттауға болады. Ұйымның әрбір қызметкері немесе тұрақты келушісі идентификаторды (электрондық кілтті) - пластикалық карточканы немесе ондағы жеке коды бар брелкаларды алады. Электрондық кілттер аталған тұлғаларды тіркеу нәтижесінде жүйе құралдарының көмегімен беріледі. Паспорттық деректер, фото (бейне бейнелеу) және электрондық кілттің иесі туралы басқа да мәліметтер дербес электрондық карточкаға енгізіледі. Иесінің дербес электрондық карточкасы және оның электрондық кілтінің коды бір-

бірімен байланысады және арнайы ұйымдастырылған компьютерлік деректер базасына енгізіледі.

Ғимаратқа немесе бақылауға жататын үй-жайға кіре берісте оқу құралдары орнатылады, олар карточкадан олардың кодын және карта иесінің қол жеткізу құқығы туралы ақпаратты оқиды және бұл ақпаратты жүйе контроллеріне береді.

Қорытындылай келгенде қол жетімді бақылау және басқару жүйесі мемлекеттік стандартқа сай төрт жүйеге бөлінеді. Қол жетімді бақылау және басқару жүйесіне төменресурсты, интернет заттарда жеңіл жұмыс істеуге биім криптографиялық алгортмдерді қолданған тиімді. Айтап айтар болсақ PHOTON, SPONGENT және Lesamanta-LW сияқты халықаралық және мемлекеттік стандарттарға сай алгоритмдер.

Қолданылған әдебиеттер тізімі

1. William J. Buchanan, Shancang Li., Rameez A., Lightweight cryptography methods // Journal of Cyber Security Technology. 05.03.2018. б 188-192.
2. Mouha N. The Design Space of Lightweight Cryptography // Journal of Cyber Security Technology. 2016. Б 25-36.
3. ISO/IEC 18033-6:2019 [ISO/IEC 18033-6:2019] IT Security techniques — Encryption algorithms — Part 6: Homomorphic encryption URL: https://www.iso.org/standard/67740.html
4. В. А. Ворона В. А. Тихонов Системы контроля и управления доступом. 2010. 13 б.
5. ГОСТ Р 51241-98 Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний URL: http://docs.cntd.ru/document/1200007411

УДК 004

МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ ЭКОЛОГИЧЕСКОЙ СИТУАЦИИ В ПРОМЫШЛЕННЫХ ЗОНАХ

Бағидолла Нұрсұлтан Маратұлы
bagidolla@gmail.com
Магистрант ЕНУ им. Л.Н.Гумилева, Нур-Султан, Казахстан
Научный руководитель – А.Тохметов

1. ЧТО ТАКОЕ МОДЕЛИРОВАНИЕ?

Моделирование – это процесс производства модели. Модель – это представление построения и работы некоторой системы интересов. Модель похожа, но проще, чем система, которую она представляет. Одной из целей модели является предоставление аналитику возможности прогнозировать влияние изменений в системе. С одной стороны, модель должна быть близка к реальной системе и включать в себя большинство ее характерных особенностей. С другой стороны, он не должен быть настолько сложным, чтобы его невозможно было понять и поэкспериментировать. Хорошая модель – разумный компромисс между реализмом и простотой.

Практики моделирования рекомендуют итеративно увеличивать сложность модели. Важной проблемой в моделировании является достоверность модели. Методы проверки модели включают моделирование модели при известных входных условиях и сравнение выходных данных модели с выходными данными системы. Обычно модель, предназначенная для имитационного исследования, представляет собой математическую модель, разработанную с помощью программного обеспечения для моделирования. Классификации математической модели включают детерминированные (входные и выходные переменные являются фиксированными значениями) или стохастические (по крайней мере, одна из входных или выходных переменных является вероятностной); статический (время не учитывается) или динамический (учитывается изменяющееся во времени взаимодействие