DOI 10.31891/2307-5732-2023-327-5-66-73
УДК: 004.67:004.4

МАРЧЕНКО ОЛЕНА
Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського»
https://orcid.org/0000-0001-5754-4920
e-mail: marchenko.helene@gmail.com

ЗАХИСТ КОНФІДЕНЦІЙНОСТІ ПЕРЕДАЧІ ТА ОТРИМАННЯ ДАНИХ ЦЕНТРУ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ (SECURITY OPERATIONS CENTER) З ВИКОРИСТАННЯМ МЕТОДІВ МІЖМАШИННОГО ЗВ'ЯЗКУ (M2M)

У роботі охарактеризовані основні потенційні проблеми та виклики, які можуть виникати між M2M-технологією та центром забезпечення безпеки при передачі та обробці даних за допомогою M2M-пристроїв. На основі проаналізованих проблем та викликів сформовані заходи щодо запобігання загроз з порушенням умов конфіденційності та цілісності даних. У роботі проводилося дослідження основних ключових параметрів для виявлення проблем захисту при передачі та отримані даних між M2M-пристроями та обладнанням центру забезпечення безпеки.

Ключові слова: безпека даних, ідентифікація, класифікація, автентифікація, SOC, M2M

MARCHENKO OLENA
National Technical University of Ukraine «Igor Sikorsky Kyiv Polytechnic Institute»

PROTECTING THE CONFIDENTIALITY OF DATA TRANSMISSION AND RECEIPT AT THE SECURITY OPERATIONS CENTRE USING MACHINE-TO-MACHINE (M2M) COMMUNICATION METHODS

The development and improvement of privacy protection technologies for data transmission and receipt is driven by the use of modern technologies that include digital equipment and auxiliary electronic media for collecting, processing and displaying information (sensors, peripherals) that can use machine-to-machine (M2M) methods for data processing by the data centre (SOC).The paper describes the main potential problems and challenges that may arise between the M2M technology and the security centre during the transmission and processing of data using M2M devices. On the basis of the analysed problems and challenges, measures to prevent threats with violation of confidentiality and data integrity are formed. In order to minimise data security threats, security measures have been developed, based on which the following were investigated: basic authorisation operations (identification, classification, authentication and data encryption); data protection and confidentiality issues with a study of the impact of DoS attacks on the M2M device system; use of software for the M2M system and SOC; M2M system planning and planning recommendations. The study investigated the main key parameters for identifying security problems in the transmission and receipt of data between M2M devices and the equipment of the security centre. Based on the literature review, the key aspects of M2M technology were analysed, where the paper addressed the issues of authorisation, encryption, monitoring, software use and scheduling. Network security threats are considered, namely: data leakage, unauthorised access, insufficient monitoring of the network and SOC systems, use of outdated and unupdated software, legal restrictions, technical circumstances from the engineering point of view. The research results showed that some research machines were subjected to DoS attacks by intruders, which indicates the search for new opportunities and methods to protect data confidentiality.

Keywords: data security, identification, classification, authentication, SOC, M2M

Вступ

Сучасні технології на основі новітніх розробок розумних систем з використанням інформаційних технологій, периферійних пристроїв та сенсорів зробили значний внесок у розвиток технології, в якій машини можуть взаємодіяти одна з одною за допомогою з'єднувальних компонентів та систем. Така технологія отримала назву M2M (Machine-to-Machine), яка дозволяє машинам, пристроям та сенсорам взаємодіяти між собою без участі людського фактору. Однак з використанням такої технології перед досвідченими розробниками, інженерами та програмістами зростає кількість нових викликів, які пов'язані з безпекою обробки, передачі та отримання даних завдяки обслуговуючим центрам безпеки даних [1, 2].

Центр забезпечення безпеки (SOC) в контексті M2M відіграє критичну роль у забезпеченні цілісності, конфіденційності та доступності даних та пристроїв. Центр забезпечення безпеки містить основні функції: проводить моніторинг безпеки (SOC відстежує активність в мережі та аналізує дані для виявлення аномалій та потенційних загроз з проведенням моніторингу діючих пристроїв); виявляє інциденти (SOC відповідає та приймає рішення на виявлені загрози та інциденти); реагує на інциденти (SOC реагує на виявлені загрози та вживає відповідних заходів для їх врегулювання, наприклад, обмежувати доступ); проводить аналіз інцидентів (SOC здійснює аналіз виявлених загроз та інцидентів для розуміння їхнього походження та визначення кращих методів для їх запобігання у майбутньому); проводить захист від атак (де SOC використовує методи та інструменти для захисту M2M пристроїв та даних від широкого спектру потенційних атак); містить ефективні методи шифрування та аутентифікації (SOC забезпечує використання ефективних методів шифрування та аутентифікації для захисту даних під час їх передачі між пристроями M2M); проводить навчання персоналу (SOC навчає персонал та операторів M2M системи виявляти загрози та діяти відповідно до стандартів безпеки [3].

Постановка проблеми

Центр забезпечення безпеки (SOC) відіграє важливе значення для обробки отриманих даних завдяки технології міжмашинної взаємодії (M2M), де отримані дані можуть зазнавати шкідливого впливу з боку зловмисників, що у свою чергу може впливати на передачу та отримання даних між машинами. Для того,

щоб дослідити основні прогалини з точки зору безпеки та конфіденційності даних необхідно проаналізувати всі можливі чинники та фактори, які можуть спричинити до витоку інформації. Тому **актуальною проблемою** даного дослідження є вивчення основних факторів ризику виникнення потенційних проблем, які пов'язані з безпекою та конфіденційністю даних. До основних проблем можна віднести наступне: фізичний доступ до пристроїв, недостатнє оновлення програмного забезпечення, мережеві загрози, недостатній рівень шифрування, управління ключами і ідентифікацією, контроль доступу та автентифікація. У даному дослідженні, авторами приділено увагу чинникам авторизації та шифрування в технології M2M.

Аналіз останніх досліджень

Технологія M2M є однією з сучасних технологій, яка привернула багато уваги як в промисловому, так і в академічному секторах й відкрила нові можливості для використання технологій Інтернету речей. Проте, існує важлива перешкода у безпеці та конфіденційності даних, яка може сповільнити зростання міжмашинної взаємодії і навіть перешкодити масовому використанню. Незважаючи на те, що було проведено безліч досліджень на тему використання технології M2M, лише деякі з них зосереджені на аспектах безпеки [4].

Від початку 2000-их років безліч аксіом вказували на те, що бездротовий зв'язок відіграватиме фундаментальну роль у забезпеченні роботи більшості додатків, які передбачатимуть повсякденне використання та поширення M2M-середовища, коли одночасно з цим стверджувалося, що безпека буде фундаментальним фактором для більшості додатків, для чого будуть потрібні відповідні методи, механізми для захисту M2M-додатків, комунікацій та користувачів. Однак у роботі [5] авторами зазначається, що бездротовий зв'язок відкриває середовище для величезних вразливостей, полегшуючи хакерам доступ до конфіденційної інформації для здійснення зловмисних дій. У роботі [6] зазначається, що механізми безпеки можуть слугувати для підтримки гетерогенних комунікаційних технологій, протоколів і пристроїв. Іншим важливим аспектом є те, що безпека повинна справлятися з автономним зв'язком між M2M-пристроями.

Для того, щоб дослідити можливість підвищення безпеки бездротового зв'язку M2M пристроїв безліч вчених розглядають питання щодо вживання відповідних заходів, які дозволяють забезпечити конфіденційність даних під час їх обробки та передачі центром забезпечення даних за допомогою бездротових технологій. Сучасні технології дозволяють передавати дані за допомогою бездротової мережі 4G LTE, де авторами у роботі [7] зазначається, що разом з вдосконалення зв'язку машинного типу (LTE-M) необхідно також досліджувати проблеми безпеки. Авторами виявлено, що проблематичним використанням мережі LTE-M може бути відсутність автентифікації з використанням карток модуля ідентифікації абонента (SIM), що потребує більш глибоко вивчення вразливих ознак для цієї вирішення проблеми. Окрім того, кожен сучасний смартфон містить міжнародний ідентифікаційний номер мобільного (IMEI), який також виконує функцію автентифікації пристрою.

Незважаючи на те, що бездротові технології мають безліч переваг, втім необхідно вдосконалювати системи безпеки, наприклад, використанням алгоритмів шифрування фізичного рівня, які досліджуються у роботі [8], шифрування з динамічними параметрами ключа для бездротового зв'язку у роботі [9], що дозволяє підвищити конфіденційність під обробки та передачі даних. Деякі рішення дозволяють впроваджувати нові можливості шифрування для M2M-пристроїв у промисловості та соціумі глобального масштабу, зокрема у роботі [10] авторами запропоновано наскрізне шифрування прозорого рівня повідомлень для телеметричного транспорту черги, що відкриває нові можливості перед індустрією 4.0.

Метою роботи є дослідження впливу проблем конфіденційності та безпеки даних при передачі та обробці даних з M2M-пристроїв центром забезпечення безпеки. Для досягнення поставленої мети сформовані наступні **задачі**: провести огляд літератури з використанням ключових аспектів авторизації та питань шифрування, моніторингу, використання програмного забезпечення та складанням планування; на основі проаналізованих джерел сформувати характерні особливості кожного з ключових аспектів з метою підвищення безпеки та вдосконаленням M2M-системи; визначити, які операції зазнають найбільшого впливу DoS-атак на M2M-систему. **Завданням** дослідження є аналіз впливу загроз на роботу M2M-системи та центру забезпечення безпеки з метою запобігання небажаних DoS-атак зловмисниками. **Предметом** дослідження є комунікаційні системи інтернету речей, які використовуються для технології передачі даних від M2M пристроїв до центру забезпечення даних.

Виклад основного матеріалу

З використанням технології міжмашинної взаємодії (M2M) можуть виникати деякі потенційні проблеми та виклики щодо захисту конфіденційності передачі та отримання даних, які обробляються центром забезпечення безпеки (Security Operations Center, скорочено SOC). До таких потенційних проблем можна віднести наступне:

- загрози мережевої безпеки, де SOC може зазнавати мережеві атаки: DDoS атаки; зламування систем ідентифікації, аутентифікації та класифікації; атаки на шифрування даних; передача та завантаження шкідливого програмного забезпечення тощо);
- витік інформації, де недостатній контроль доступу, недостатнє шифрування та помилки в налаштуванні можуть призвести до витоку конфіденційності даних в SOC;
- несанкціонований доступ, де внутрішні загрози від співробітників або сторонніх агентів можуть призвести до незаконного доступу до даних SOC;
- недостатній моніторинг мережі та систем SOC, що може призвести до непомітного виявлення

аномалій та загроз конфіденційності даних;

- використання застарілого та неоновленого програмного забезпечення, що може слугувати в якості джерела вразливості;
- законодавчі обмеження, де деякі закони та регуляції можуть вимагати дотримання певних стандартів, що у свою чергу може обмежувати обробку та передачу даних у SOC;
- технічні обставини з точки зору інженерії, де зловмисники мають на меті ввести в оману обслуговуючий персонал (співробітників SOC) для отримання доступу до даних

Тому для забезпечення конфіденційності необхідно ретельно проаналізувати потенційні проблеми та завчасно вжити заходів для ефективного вирішення можливих проблем. До основних заходів захисту конфіденційності передачі та отримання даних у центрі забезпечення безпеки з використанням методів M2M можуть вживатися заходи, які зазначені у табл. 1.

Таблиця 1

Вживання заходів безпеки конфіденційності передачі та отримання даних

Назва заходу	Пояснення	Приклади та дослідження
Шифрування даних	Для забезпечення конфіденційності даних під час їх передачі між M2M пристроями та SOC використовують протоколи, які здатні підтримувати шифрування на різних рівнях даних.	Стандарт шифрування (AES) [11]; Програмно-апаратний шифр (HW/SW) [12]; шифрування корисного навантаження P2S та P2B [13]; OTP (D-OTP) [14].
Віртуальні приватні мережі (VPN)	Для створення безпечного тунелю між M2M пристроями та SOC використовується VPN, що дозволяє та забезпечує зашифровано передавати дані.	Підходи VPN IPSec/IPv6 та OpenSSL для безпеки Hybrid End-to-End VPN [15]; OpenVPN і IPsec [16]
Авторизація та автентифікація	Авторизація вимагає взаємної автентифікації M2M пристроїв та SOC з метою довіреності та взаємодії між декількома пристроями та користувачами.	Ефективне виявлення та класифікація типів пристроїв (EDDC) [17]; протокол SLAP (безпечний та легкий протокол автентифікації) [18]
Моніторинг безпеки	Використання систем моніторингу дозволяють виявляти аномалії та можливі загрози у мережі M2M.	Датчики для температури (RTD PT-100, LM35 [19]
Захист від атак	Використання заходів безпеки, а саме брандмауери та системи виявлення вторгнень для захисту мережі M2M та SOC від атак.	Firewall Management Software, Intrusion Detection System/Intrusion Prevention System (IDS/IPS) [20]
Фізична безпека	Забезпечення фізичного захисту пристроїв M2M та обладнання SOC для уникнення фізичного доступу несанкціонованим особам (за допомогою міжмашинних вузлів).	Атаки на побічні канали, фальсифікація вузлів, модифікація програмного забезпечення, апаратні трояни, знищення M2M-пристроїв
Постійне оновлення	Обладнання та програмне забезпечення M2M та SOC необхідно оновлювати та підтримувати в актуальному стані з метою виправлень відомих вразливостей.	Arduino IDE, Raspberry Pi [21], PlatformIO, Python, Node-RED, Microsoft Azure IoT, AWS IoT, Google Clout IoT
Аудит та планування	Розробка плану на випадок порушення конфіденційності даних та відновлення нормальної роботи. Ведення журналів подій для моніторингу та аналізу активності M2M пристроїв з метою завчасного реагування на можливі загрози. Планування на основі алгоритмів	Пропорційна справедливість (PF), експоненційно-пропорційна справедливість (EXP/PF), перша найбільша зважена затримка (MLWDF), планувальник на рівні кадру (FLS), експоненційне правило (EXP-RULE) та логарифмічне правило (LOG-RULE) [22]

Джерело: сформовано автором на основі [11–22]

Методика експериментальних досліджень полягає в обґрунтуванні основних проблем захисту та передачі даних на основі міжмашинної взаємодії (M2M), які підлягають обробці центром безпеки даних. На основі проаналізованих останніх джерел можна зробити припущення, що кожна потенційна проблема може вирішуватися завдяки вживанню заходів безпеки конфіденційності передачі та отримання даних. Розглянемо коротко основні параметри, які здатні впливати на роботу M2M пристроїв.

Шифрування

Шифрування даних в центрі забезпечення безпеки M2M є критичним для захисту конфіденційності та цілісності інформації, якою можуть обмінюватися машини завдяки технології M2M. Розглянемо декілька ключових аспектів шифрування даних.

1. Використання ефективного шифрування, що дозволяє використовувати сучасні та безпечні

алгоритми шифрування, наприклад AES (Advanced Encryption Standard). Однак варто зауважити, що використання ключів з відповідною довжиною та правильним управлінням ключами також є критичним.

2. Керування ключами, де ключі шифрування повинні бути належно керованими. Використання системи керування ключами для створення, обміну та обновлення ключів є важливим елементом безпеки.

3. Захист ключів і ідентифікація є важливим для забезпечення фізичного та логічного захисту ключів шифрування. Перевірка ідентичності пристроїв, які обмінюються даними відіграє важливу роль у забезпеченні безпеки.

4. Безперебійне та постійне шифрування, де дані повинні шифруватися між машинами та центром забезпечення безпеки під час передачі. Використання протоколів, таких як TLS (Transport Layer Security), може бути корисним для забезпечення безпеки комунікацій.

5. Моніторинг та аудит безпеки: Важливо здійснювати моніторинг і аудит безпеки, щоб вчасно виявляти та реагувати на можливі загрози.

Етапи авторизації

Ідентифікація M2M пристроїв на основі кластеризації. Процес кластеризації виконується в автономному режимі для того, щоб визначити, який вузол є головним кластером (ГК), а який вузол є другорядним кластером (ДК). Після цього вузли можуть класифікуватися як справжні та атаковані пристрої на основі характеристик оцінки довіри (ОД) для того, щоб оптимізувати процес кластеризації. Використовуючи ці вагові коефіцієнти обчислюється значення показника довіри в діапазоні від 0 до 1. Атаковані пристрої оновлюють список ОД, тоді як легітимні пристрої оновлюють список ГК. Щоб обчислити ГК для певного інтервалу, обчислюється значення ОД кожного вузла в списку ГК з періодичним інтервалом. Інтервал часу передачі даних рекламується і оголошується призначеним ДК. На кожному інтервалі перевіряється залишок енергії для СН і кластерний цикл модифікується [17].

У комунікаціях M2M пристроїв, протоколи авторизації використовуються для ідентифікації та класифікації пристроїв. Як правило, протокол повинен базуватися на визначенні типу пристрою і повинен містити в собі етап ідентифікації, на якому обчислюється періодичне значення ОД для кожного вузла. Спочатку обчислюється та ідентифікується показник довіри (ПД). Вузол ідентифікується як неідентифікований пристрій, якщо його значення ПД більше, ніж глобальне порогове значення ОД. В іншому випадку вузол може бути ідентифікований як атакований пристрій [16-17].

Класифікація пристроїв M2M. Після алгоритму ідентифікації, введення пристроїв та даних для класифікації пристроїв є наступним етапом. Алгоритм може використовувати значення ОД, яке регулярно обчислюється, при цьому кожен сенсорний вузол ідентифікується і приймається легітимними пристроями та вузлами, які є вразливими до атак зловмисного програмного забезпечення. ПД повинен розраховуватися для кожного вузла у мережі з використанням даних коефіцієнту доставки та отримання.

Щоб розпочати процес класифікації, кластери, що складаються з ГК та ДК необхідно спочатку класифікувати. Легітимні вузли розглядаються для подальшого вибору ГК, в той час, коли заражені шкідливим програмним забезпеченням вузли слугують в якості ДК. Для кожного вузла обчислюється ОД, після чого обирається ГК у мережі на основі значення довіри. Центральна станція вказує на максимальне споживання енергії, оскільки вона повинна бути активною весь час під час процесу передачі даних [17, 25].

Автентифікація та шифрування пристроїв. Після етапу реєстрації кожен датчик підлягає автентифікації на маршрутизаторі. Варто зазначити, що під час процедури автентифікації датчик ніколи не використовує свій справжній ідентифікатор для автентифікації на маршрутизаторі. Таким чином, ідентифікатор розумного датчика не може бути підслуханий зловмисником [11].

Розглянемо верифікацію з використанням комбінування технологій автентифікації та шифрування. Використання інструменту формальної верифікації програмного забезпечення з відкритим кодом Simple Promila Interpreter (SPIN) застосовується для формальної верифікації більшості програмних додатків [23]. На рис. 2 показано процес автентифікації між пристроями зв'язку машинного типу (ПЗМТ) за допомогою довіреного сервера, де ПЗМТ 2 дорівнює (ключ 1450) й надсилається на довірений сервер (ДС). На основі ідентифікатора ДС повертає відкритий ключ MTCD 2 на MTCD 1, підписаний ДС (ключ 360)

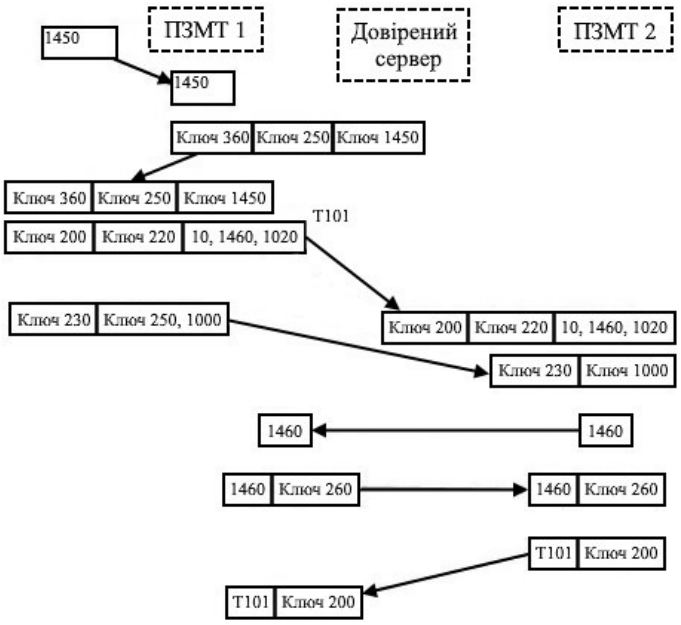

Рис. 2. Схема автентифікації в M2M системах з використанням шифрування
Джерело: сформовано автором на основі [24]

Як тільки ПЗМТ 1 отримує ключ, він може перевірити підпис з підтвердженням ДС, що відкритий ключ належить ПЗМТ 2. Після цього, ПЗМТ 1 генерує спільний секретний ключ (ключ 200) – спільну пару з відкритим та закритим ключами (220), які надсилаються до ПЗМТ 2. У разі потреби ПЗМТ 2 може перевірити підпис ДС та запросити відкритий ключ у ПЗМТ 1 для розшифрування секретного ключа. Як тільки він отримає відкритий ключ ПЗМТ 1, він розшифровує спільний секретний ключ. Така схема автентифікації здатна захистити систему від атак повторного відтворення та імітацій [23].

Дослідження впливу DoS-атак на систему M2M-пристроїв

Для того, щоб продемонструвати роботу центру забезпечення безпеки з технологією передачі даних між M2M пристроями, в якості прикладу розглянемо модель у роботі [25], в якій розглядаються комунікаційні операції M2M-пристроїв для обробки даних головною машиною у SOC. На рис. 2 представлено систему взаємозв'язку M2M-пристроїв з виконанням операцій центром забезпечення безпеки, в якій комунікаційні системи (датчики та вимірювальні прилади) підключені до єдиної системи в режимі реального часу й працюють в автономному режимі.

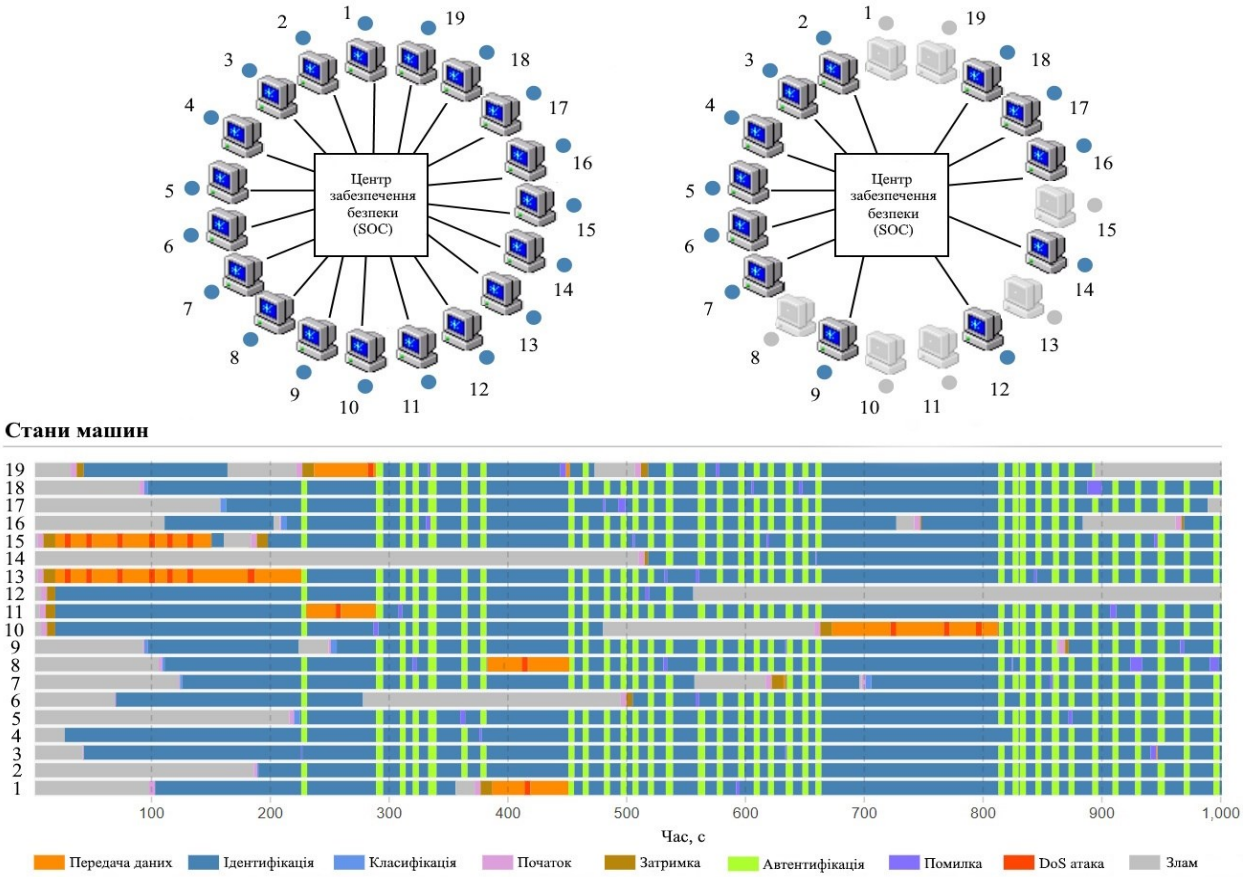

Рис. 2. Система взаємозв'язку M2M-пристроїв з виконанням операцій центром забезпечення безпеки.
Джерело: сформовано автором на основі [25]

За структурою управління така M2M система складається з 19 машин, де кожна машина містить в собі M2M-сервер, основну мережу, M2M-мережу та датчики. Сервери з'єднані між собою й підключені до операційного центру безпеки.

Запуск машини та автентифікація здатні забезпечувати безпеку машин та зберігати дані, але можуть впливати на затримку M2M-звя'зку. Тому в окремих випадках зловмисники можуть скористатися такою ситуацією та обійти процес автентифікації, що у свою чергу може вплинути на продуктивність машини та системи в цілому. Складні алгоритми перевірки пов'язані з помилками, які найчастіше виникають під час процесу автентифікації. Ці алгоритми засновані на використанні алгебраїчних формул і алгоритмів шифрування, які можуть призвести до помилок, якщо машина працює неправильно під час обробки даних. Атака на відмову в обслуговуванні (DoS атака) є атакою на комп'ютерну систему з використанням шкідливого ПЗ, яка призводить до збою та аварійного завершення роботи системи.

На рис. 2 можна побачити дві ідентичні схеми за участі 19 машин, які обробляються головною машиною з відповідним обладнанням у SOC. Одна схема (ліворуч) демонструє активний стан робити системи в спільному середовищі SOC, а інша схема демонструє машини, які зазнали впливу зловмисників й були виведені з ладу через атаку з використанням шкідливого ПЗ, що врешті-решт могло призвести до витоку даних та порушення умов конфіденційності та безпеки. Тому окрім операцій авторизації та шифрування даних необхідно також приділяти увагу моніторингу за машинами, які задіяні у даній технологій з M2M-пристроями.

Розглянемо захист конфіденційності передачі даних згідно рис. 2., де машини 1, 8, 10, 11, 13, 15 та 19 здійснюють передачу даних й одночасно з цим відбуваються різні операції, включаючи операції ідентифікації, класифікації та автентифікації. Машини 11 і 19 зазнали короткої DoS-атаки з витоком даних тривалістю від 200 до 300 с на початку процесу автентифікації. Аналогічно, машини 1 і 8 повторно пройшли автентифікацію між 400 і 450 с, що призвело до короткого витоку даних. З перелічених машин видно, що машина під номером 19 піддається DoS-атаці, після чого машина продовжує працювати й зазнає зламу системних файлів, коли машина під номером 15 після DoS-атаки закінчила свою роботу й відновила її. Варто зауважити, що машина під номером 13 зазнала 7 спроб DoS-атаки, але зловмисникам не вдалося зламати систему, коли машина під номером 19 зазнала лише 1 DoS-атаки й піддалася зламуванню системи. За кількістю DoS-атак машин під номером 13 та 15 можна зробити припущення, що якщо за проміжок часу в 200 с не прийняти відповідних рішень, то система цих машин може призвести до витоку даних. Кожна несподівана атака шкідливого програмного забезпечення запускала процес автентифікації. Машина 10, яка вийшла з ладу в результаті операції зазнала тричі DoS-атаки на систему в проміжку часу від 650 до 790 с після перезавантаження системи, що призвело до витоку даних.

Аналіз можливостей та використання ПЗ для M2M та SOC

Для розробки та впровадження програмного забезпечення для M2M та SOC існують різні інструменти та платформи. Розглянемо основні програми та платформи, які можуть використовуватися для розробки M2M-рішень та забезпечення конфіденційності даних SOC у табл. 2.

Таблиця 2

Аналіз ПЗ для M2M та SOC

M2M	SOC
Arduino IDE (застосовується у випадках потреби використання мікроконтролера Arduino у випадках для розробки програми для M2M-пристроїв на платформі Arduino).	**SIEM** (системи, які допомагають агрегувати, аналізувати та моніторити події безпеки з різних джерел, такі як файли журналів, сенсори та системи виявлення вторгнень (IDS/IPS)).
Raspberry Pi: Raspberry Pi (містить набір інструментів та середовище для розробки програм M2M-пристроїв).	**IDS/IPS** (системи, які слідкують за надзвичайною або підозрілою активністю в мережі й можуть виявляти вторгнення).
PlatformIO (відкрите середовище для розробки вбудованого програмного забезпечення, яке підтримує багато різних мікроконтролерів та платформ, включаючи Arduino, ESP8266, ESP32).	**Firewall Management Software** (допомагає в налаштуванні та керуванні брандмауерами для фільтрації трафіку та забезпечення безпеки мережі).
Python (використовується для розробки M2M-рішень через бібліотеки та фреймворки, такі як Twisted, MQTT, і багато інших).	**Елементи керування доступом IAM** (допомагають в управлінні доступом користувачів до ресурсів та систем).
Node-RED (використовується для розробки M2M-рішень, що дозволяє зв'язувати та налаштовувати взаємодію між пристроями через візуальний інтерфейс).	**Управління подіями та реагування на інциденти ERM** (використовується для координації та відслідковування інцидентів та відгуку на них).
Microsoft Azure IoT (містить широкий спектр інструментів для розробки та управління M2M-ріщеннями, включаючи IoT Hub, Azure Functions, і Power BI для аналітики даних).	**Аналіз безпеки (п**рограми для аналізу даних та ідентифікації загроз безпеці, використання антивірусного та анти-шпигунського програмного забезпечення та корпоративних інструментів SOC.
AWS IoT: Amazon Web Services (містить платформу для розробки M2M-рішень, що включає IoT Core, Greengrass та інші сервіси).	**Конфігураційне управління та автоматизація CMA** (допомагає в налаштуванні і керуванні конфігураціями систем та пристроїв).
Google Cloud IoT (містить інструменти та сервіси для створення M2M-рішень на основі Google Cloud).	**Інструменти для виявлення та аналізу загроз TDAT** (допомагає виявляти та аналізувати нові загрози безпеки).

Джерело: сформовано автором на основі [15–20]

Планування для системи M2M

Ведення журналів (параметр логування) та розробка плану для системи M2M допомагають забезпечити ефективне функціонування та моніторинг мережі. Розглянемо коротко кожен крок планування для системи M2M у табл. 3.

Проаналізувавши рекомендації щодо планування систем M2M можна зробити припущення, що під час дослідження на рис. 2 кожна машина та пристрої передачі даних повинні мати механізми автоматичного збору інформації для ведення журналів, а також повинні містити аналітичні інструменти та алгоритми, які зможуть забезпечити передвчасне виявлення вторгнень у систему та аномальну активність. Тому для кожної машини на рис. 1 потрібно проводити: шифрування журналів, моніторинг статусу пристроїв та мережі M2M, план для відновлення послуг у випадку збоїв та атак, ідентифікацію та автентифікацію для забезпечення доступу до мережі довірених пристроїв тощо.

Таблиця 3

Кроки планування та рекомендації щодо планування до системи M2M

№	Крок планування	Пояснення та рекомендації щодо планування
1	Ведення журналів	Необхідно: визначити, які події та дії в мережі M2M слід ввести в журнал; вибрати спеціалізовані системи для логування, наприклад, інформацію про безпеку та управління подіями (ІБУП) для агрегації та аналізу журналів; забезпечити стандартизацією формату журналів й регулярні аудиторські рецензії для виявлення аномалій).
2	Збір та аналіз журналів	Необхідно встановити механізми автоматичного збору журналів з усіх пристроїв та компонентів M2M; використовувати аналітичні інструменти та алгоритми для виявлення вторгнень, аномальної активності тощо; розробити процедури реагування на виявлені аномалії.
3	Захист даних журналів	Необхідно: проводити шифрування журналів та забезпечити контроль доступу до них; зберігати журнали в надійних та захищених сховищах.
4	Автоматизація моніторингу	Необхідно: розробити системи для автоматичного моніторингу статусу пристроїв та мережі M2M; встановити автоматичні повідомлення та реакції на виникнення проблем.
5	План надійності та відновлення	Необхідно розробити план для відновлення послуг у випадку збоїв або вторгнень, забезпечити створення регулярних резервних копій конфігурації та даних пристроїв M2M.
6	Спостереження за зростанням мережі	Необхідно постійно оцінювати потреби та розширення мережі M2M, включаючи нові пристрої та з'єднання.
7	Ідентифікація та автентифікація пристроїв	Необхідно використовувати механізми ідентифікації та автентифікації для забезпечення доступу до мережі M2M довірених пристроїв.

Джерело: Сформовано автором на основі [26]

Висновки

У роботі охарактеризовані основні потенційні проблеми та виклики, які можуть виникати між M2M-технологіями та центром забезпечення безпеки, де було з'ясовано, що кожна проблема зазнає негативного впливу на функціонування M2M-системи. Розглянуто загрози мережевої безпеки, а саме: витік даних, несанкціонований доступ, недостатній моніторинг мережі та систем SOC, використання застарілого та неоновленого програмного забезпечення, законодавчі обмеження, технічні обставини з точки зору інженерії. З метою мінімізації загроз з питань безпеки даних сформовані заходи безпеки, на основі яких було досліджено: основні операції авторизації (ідентифікація, класифікація, автентифікація та шифрування даних); проблеми захисту та конфіденційності даних з дослідженням впливу DoS-атак на систему M2M-пристроїв (див. рис. 2); використання програмного забезпечення для M2M-системи та SOC; планування M2M системи та рекомендації щодо планування.

Вживання заходів безпеки конфіденційності передачі та отримання даних між M2M-пристроями та SOC охарактеризували основні операції, які відіграють важливе значення для функціонування M2M-системи, наприклад, авторизація, шифрування та моніторинг є найважливішими факторами, які здатні впливати на роботу системи, однак оновлення компонентів програмного забезпечення має бути постійним та автоматизованим, що зможе покращити захист від атак та підвищити фізичну безпеку обладнання та пристроїв. Під час дослідження авторами з'ясовано, що на рис. 2 деякі машини могли зазнати значної шкоди через DoS-атаки, що могло призвести до аварійних відключень. Тому під час проєктування, обслуговування та ремонту пристроїв з обладнанням необхідно постійно вдосконалювати системи, щоб мінімізувати ризики, які можуть спричинити витік даних.

Результати досліджень показали, що з наявних 19 машин – 7 машин зазнали зловмисних DoS-атак зловмисниками, що свідчить про застарілість методів захисту, або використання застарілого програмного забезпечення. Проаналізувавши всі чинники та фактори використання M2M-технології можна зробити висновок, що разом з вдосконаленням технологій та програмного забезпечення розвиваються також шкідливі системні програми та віруси, якими зловмисники можуть завдати сильних збитків на систему обробки даних й поставити під загрозу конфіденційність та безпеку передачі даних. Деякі параметри M2M-системи можуть призвести також до незначних затримок роботи у часі, що також свідчить про стан кожної окремої машини.

References

1. Mirani A.A., Velasco-Hernandez G., Awasthi A., Walsh J. Key Challenges and Emerging Technologies in Industrial IoT Architectures: A Review. Sensors. 2022, 22(15). P. 36.

2. Zhou Z., Guo Y., He Y., Zhao X., Bazzi W.M. Access control and resource allocation for M2M communications in industrial automation. IEEE Transactions on Industrial Informatics, 15(5), 2019. P. 3093-3103.

3. Zhong Y. Real-Time Monitoring Systems that Provide M2M Communication between Machines. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences. 2023.

4. Tagarev T., Sharkov G. Computationally intensive functions in designing and operating distributed cyber secure and resilient systems. In Proceedings of the 20th International Conference on Computer Systems and Technologies. 2019. P. 8

5. Lokhande M.P., Patil D.D. Network performance measurement through machine-to-machine communication in tele-robotics system. Tehnički glasnik. 2002, P. 98.

6. Granjal J., Monteiro E., Silva J. S. Security issues and approaches on wireless M2M systems. Wireless Networks and Security: Issues, Challenges and Research Trends. 2013, P. 133.

7. Yang T.W. Achieving M2M-device authentication through heterogeneous information bound with USIM card. Future Generation Computer Systems. 2022, 110, P. 629.

8. Noura H., Melki R., Chehab F., Mansour M.M., Martin S. Efficient and secure physical encryption scheme for low-power wireless M2M devices. In 2018 14th International Wireless Communications & Mobile Computing Conference (IWCMC). 2018, P.1267, IEEE.

9. Noura H. N., Melki R., Chehab A., Mansour M.M. A physical encryption scheme for low-power wireless M2M devices: a dynamic key approach. Mobile Networks and Applications. 2019, P. 447.

10. Gupta S., Sacchetti T., Crispo B. End-to-End Encryption for Securing Communications in Industry 4.0. In 2022 4th IEEE Middle East and North Africa COMMunications Conference (MENACOMM). 2022. 158 p. IEEE.

11. Karacan E., Akleylek S., Karakaya A. Pq-flat: a new quantum-resistant and lightweight authentication approach for m2m devices. In 2021 9th International Symposium on Digital Forensics and Security (ISDFS). 2021. 5 p., IEEE.

12. Bahadori M., Järvinen K. A programmable SoC-based accelerator for privacy-enhancing technologies and functional encryption. IEEE Transactions on Very Large Scale Integration (VLSI) Systems. 2020, 28(10), 2195 p.

13. Mathews S. P., Gondkar R. R. Protocol recommendation for message encryption in MQTT. In 2019 International Conference on Data Science and Communication (IconDSC). 2019, 1 p., IEEE.

14. Tsai W.C., Tsai T.H., Wang T.J., Chiang M.L. Automatic Key Update Mechanism for Lightweight M2M Communication and Enhancement of IoT Security: A Case Study of CoAP Using Libcoap Library. Sensors. 2022, 22(1), 340 p.

15. Juma M., Monem A.A., Shaalan K. Hybrid end-to-end VPN security approach for smart IoT objects. Journal of Network and Computer Application. 2020, 158 p., 102598.

16. Ghanem K., Ugwuanyi S., Hansawangkit J., McPherson R., Khan R., Irvin J. Security vs bandwidth: performance analysis between IPsec and OpenVPN in smart grid. In 2022 International Symposium on Networks, Computers and Communications (ISNCC). 2022, 1 p., IEEE.

17. Lokhande M.P., Patil D., Shabaz L.V. Machine-to-machine communication for device identification and classification in secure telerobotics surgery. Security and communication networks. 2021, 1-16 p.

18. Panda S., Mondal S., Kumar N. SLAP: A Secure and Lightweight Authentication Protocol for machine-to-machine communication in industry 4.0. Computers & Electrical Engineering. 2022, 98 p., 107669.

19. Saravia M., Salvador R., Palencia C., Zepeda A. Monitoring system for solar thermal station with IoT and M2M. In 2017 IEEE 37th Central America and Panama Convention (CONCAPAN XXXVII). 2017, 1-6 p., IEEE.

20. Mahboub S.A., AhmedR E. Smart IDS and IPS for cyber-physical systems. In Artificial intelligence paradigms for smart cyber-physical systems. 2021, 109-136 p., IGI global.

21. Imani A., Keshavarz-Haddad A., Eslami M., Haghighat J. Security challenges and attacks in m2m communications. In 2018 9th International Symposium on Telecommunications (IST). 2018, pp. 264-269. IEEE

22. Ouaissa M., Rhattoy A., Lahmer M. Comparative performance study of QoS downlink scheduling algorithms in LTE system for M2M communications. In Information Systems and Technologies to Support Learning: Proceedings of EMENA-ISTL. 2018, 216-224 p. Springer International Publishing.

23. Kakinada J.N.T., Pradesh A. Implementation of a Group-Based Verification Mechanism for Secure M2M Communications. J. Univ. Shanghai Sci. Technol. 2020, 22(12), 78-92 p.

24. Murthy B.S., Sumalatha L. A distributed authentication and key exchange approach for secure M2M communications. In 2017 3rd International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT). 2017, 277 p. IEEE.

25. Zhong Y. Real-Time Monitoring Systems that Provide M2M Communication between Machines. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences. 2023.

26. Jayachandran M., Reddy C.R., Padmanaban S., Milyani A.H. Operational planning steps in smart electric power delivery system. Scientific Reports. 2021, 11(1), 17250.