УДК: 001-004.7

ОЦІНЮВАННЯ ПОВЕРХНІ АТАК ЕЛЕКТРОННИХ КОМПОНЕНТІВ УПРАВЛІННЯ АВТОМОБІЛЯ В МЕРЕЖІ CAN

Чеканін О. Ю.,

кандидат технічних наук, доцент, Жданова О. Г.

Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», Україна, Київ

Предметом роботи є підхід до кількісного оцінювання інформаційної безпеки комп'ютерної мережі автомобіля та електронних компонент управління (ЕКУ), що передають дані нею. Метою є надання кількісної оцінки поверхні атак для ЕКУ автомобіля, що використовують протокол передачі даних CAN. Для досягнення мети були адаптовані терміни та поняття загальна методологія оцінювання поверхні атаки для використання по відношенню до ЕКУ автомобіля, проаналізовані зусилля зловмисника для отримання доступу до ресурсів в рамках здійснення атаки. Був наданий опис загальних типів атак та побудовані дерева атаки для них. Запропоновано спосіб оцінювання поверхні атак з використанням діагностичних функцій та атак з використанням нормальних пакетів. Цей спосіб базується на використанні оцінок величин потенційних збитків від атак та оцінок зусиль для доступу да каналів, даних та методів ЕКУ. Результатом є оцінка поверхні атак для ЕКУ, яка характеризує ступінь вразливості ЕКУ до здійснення атак. Ця інформація важлива для виробників транспортних засобів для здійснення заходів з підвищення рівня інформаційної безпеки.

Ключові слова: інформаційна безпека автомобіля, поверхня атаки, зусилля зловмисника, потенційні збитки, дерево атаки, оцінка поверхні атаки.

Чеканин А. Ю., кандидат технических наук, доцент, Жданова Е. Г. Оценивание поверхности атак электронных компонентов управления автомобиля в сети CAN / Национальный технический университет Украины «Киевский политехнический институт имени Игоря Сикорского», Украина, Киев

Предметом работы является подход к количественному оцениванию информационной безопасности компьютерной сети автомобиля и электронных компонентов управления (ЭКУ), которые обмениваются данными по ней. Целью является предоставление количественной оценки поверхности атак для ЭКУ автомобиля, которые используют протокол передачи данных CAN. Для достижения цели были адаптированы термины и общая методология оценивания поверхности атаки для использования по отношению к ЭКУ автомобиля, проанализированы усилия злоумышленника для получения доступа к ресурсам в рамках осуществления атаки. Было представлено описание общих типов атак и построены деревья атаки для них. Предложен способ оценивания поверхности атаки с использованием диагностических функций и атак с использованием нормальных пакетов. Способ базируется на использовании оценок величины потенциального ущерба от атак и оценок усилий для доступа к каналам, данным и методам ЭКУ. Результатом является оценка поверхности атак для ЭКУ, которая характеризует степень уязвимости ЭКУ к осуществлению атак. Эта информация является важной для производителей транспортных средств для осуществления мер по повышению уровня информационной безопасности.

Ключевые слова: информационная безопасность автомобиля, поверхность атаки, усилия злоумышленника, потенциальные убытки, дерево атаки, оценка поверхности атаки.

O. Chekanin, Ph.D. in Technical Science, O. Zhdanova Assessment of attack surface for vehicle electronic control units in CAN network / National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute" Ukraine, Kyiv

The subject of the paper is the approach to the quantitative assessment of information security of the vehicle computer network and electronic control units (ECUs) that exchange data via this network. The goal is to provide a quantitative assessment of the attack surface for vehicle ECUs that use the CAN data protocol. The terms and general methodology for assessing the attack surface were adapted for use concerning the vehicle's ECUs to achieve the goal, the efforts of the attacker to gain access to resources within the framework of the attack were analyzed. A description of the general types of attacks was presented, and attack trees were built for them. A method for assessing the attack surface using diagnostic functions and attacks using normal packets is proposed. The method is based on the use of estimates of the potential damage magnitude from attacks and assessments of efforts to access the channels, data, and methods of the ECU. The result is an assessment of the attack surface for the ECU, which characterizes the degree the ECU is vulnerable to the attack. This information is essential for vehicle manufacturers for implementing measures to improve the level of information security.

Keywords: vehicle security, attack surface, attacker's effort, potential damage, tree attack, attack surface estimation.

Вступ. Поверхня атак [1,2] — це сукупність усіх точок входу (векторів атак) в систему, за допомогою яких неавторизований користувач (зловмисник) може впровадити власні дані, вилучити дані або ініціювати подію, прав на яку він не має. Однією з методик забезпечення безпеки захищуваної системи є утримування поверхні атак в визначених межах.

Поверхня атак визначає, які частини системи потребують перегляду та тестування на наявність вразливостей системи безпеки. Мета аналізу поверхні атаки полягає в тому, щоб зрозуміти зони ризику в захищуваній системі, щоб розробники та спеціалісти з безпеки знали, які частини програми відкриті для атак, могли знайти способи мінімізувати це, і помітити, коли і як поверхня атаки змінюється і що це означає з точки зору оцінки ризиків.

Розділяють поверхні атак для програмного забезпечення, мереж та людську. В залежності від контексту, цей термін має відповідне значення. В даній роботі розглядається поверхня атак для мереж CAN у складі автомобіля.

Чисельні атаки на ЕКУ автомобіля підтвердили наявність вразливостей в існуючих рішеннях, які проектувалися без урахувань інформаційної безпеки. Поверхня атак є інструментом аналітиків, що показує сукупність можливих шляхів здійснення неавторизованих дій по відношенню до захищуваної системи.

Створенням поверхні атак займається група експертів з інформаційної безпеки, які на власний розсуд визначають можливі атаки та надають пріоритети. Також варто зазначити, що більшість робіт з отримання метрик та алгоритму складання поверхні атак зосереджені виключно на системах, які аналізуються. Тобто використання методики, що добре підходить до файлових систем

може бути неможливим по відношенню до іншого програмного забезпечення, наприклад ERP систем.

В роботі використовується загальна методика оцінювання поверхні атак[2], яка була застосована до програмного забезпечення серверів протоколу IMAP: Courier-IMAP та Cyrus та одного із компонентів системи SAP - SAP NetWeaver. Ця методика розрахована на програмне забезпечення, тому необхідно адаптувати її до використання по відношенню до CAN мережі та елементів мережі.

Ключовими поняттями в методиці є: канали, сховище даних, методи.

Під каналом розуміється будь-який канал зв'язку з мережею, який використовує зловмисник. Це може бути відкритий порт, сокет, підмережа в мережі. Під сховищем даних розуміється сукупність даних, які існують постійно або тимчасово. До даних, які зберігаються постійно належать файли, записи бази даних. Тимчасові дані — це дані, що існують в пам'яті процесу, що виконується, тощо. Методами є функціональність, яку елемент мережі може виконати. Це може бути реакція на дані, що надійшли з мережі, робота самого елемента мережі згідно з його призначенням, тощо.

Необхідно зазначити, що канали, методи та сховища даних розглядаються як ресурси. Не всі ресурси однаково впливають на оцінку поверхні атак мережі, оскільки не всі ресурси однаково ймовірно будуть використані зловмисником. Внесок ресурсу до поверхні атаки системи залежить від потенціального збитку, тобто рівня шкоди, який зловмисник може заподіяти під час використання ресурсу в атаці та зусиль, які зловмисник витрачає на придбання необхідних прав доступу, щоб мати можливість використовувати ресурс в атаці. Чим вище потенційний збиток або чим менше зусилля, тим вище внесок у поверхню атак.

Постановка задачі. В роботах [3-5] автори зосереджені на пошуку практичної можливості здійсненні неавторизованих дій в мережі автомобіля, дослідники[6] надили опис поверхні атак для ЕКУ за результатами атак, проте вони дають лише опис можливих наслідків. Задачею цією статті є створення кількісної оцінки для поверхні атак ЕКУ за результатами здійснених атак. Аналіз атак дає можливість виділити типові варіанти здійснення зловмисних дій і для кожного з них створено дерево атаки для послідовного опису дій.

Оцінювання атак на ЕКУ. Кожен ЕКУ [7] може бути об'єктом декількох атак, кожна з яких спричиняє різні наслідки на функціональність автомобіля, безпеку водія та пасажирів та керування. Одна й та ж сама атака, здійснена по відношенню до двох різних ЕКУ відрізнятиметься в наслідках через те, що кожен ЕКУ відповідає на певну частину функціональності автомобіля. Тому має сенс оцінити саме ЕКУ, а не атаки. Оцінка показуватиме важливість ЕКУ з точки зори безпеки у разі здійснення атак.

Під оцінкою атаки будемо розуміти відношення потенційного збитку до докладених зусиль [2]:

$$S_{ECU} = \frac{\sum_{i=1}^{n} T_i}{E_c + E_d + E_m} \qquad (1)$$

де n- кількість виявлених загроз для оцінюваного ЕКУ;

T_i – оцінка *i*-ї загрози – величина потенційного збитку (встановлюється експертами з питань інформаційної безпеки автомобіля);

E_c – оцінка зусиль для доступу до каналу, який використовує ЕКУ (експертна оцінка);

E_d – оцінка зусиль для доступу до даних ЕКУ (експертна оцінка);

E_m – оцінка зусиль для виклику методів в ЕКУ (експертна оцінка).

Зусилля, які зловмисник витрачає, наприклад, на відкриття діагностичної сесії можуть дозволити провести йому більше однієї атаки. Тобто зусилля, які були витрачені один раз, дозволяють нанести максимальний збиток в межах отриманого доступу. В такому випадку, зусилля потрібно враховувати лише один раз, тоді як потенційний збиток враховується за кожну атаку. Тож в формулі (1) E_c, E_d та E_m - це оцінки унікальних зусиль для виконання усіх атак на розглянутий ЕКУ.

Оцінювання зусиль для доступу до каналів. В роботі [6] показано, що зловмисник може отримати доступ до CAN мереж автомобіля через канали фізичного доступу, канали близької відстані та канали дальньої відстані. Доступ до кожного каналу вимагає від зловмисника різних зусиль та дає різні можливості.

Канали фізичного доступу вимагають безпосередньої взаємодії з обладнанням автомобіля, що може бути ускладнено або неможливо. Також існує загроза того, що зловмисника помітять. Прикладами є OBD-II порт, CD програвач, USB порт, порт підключення мобільного пристрою, пристрій для діагностики.

Канали близької відстані дозволяють зловмиснику отримати доступ, знаходячись поруч без ризику бути поміченим. Приклади: Bluetooth, Wi-Fi.

Канали дальньої відстані дозволяють зловмиснику отримати доступ, знаходячись в будь-якому місці, проте вимагають найбільших зусиль. До каналів дальньої відстані відноситься стільниковий зв’язок.

В рамках роботи вважається що фізичний доступ вимагає найменших зусиль, а доступ через канали дальньої відстані – найбільших зусиль. Таким чином запропоновано таке ранжування значень оцінок:

– оцінка зусиль для фізичного доступу складає $E_{physical} = 1$,

– оцінка зусиль доступу до каналів близької відстані складає $E_{short-range} = 5$,
– оцінка зусиль доступу до каналів дальньої відстані складає $E_{long-range} = 10$.

Очевидно, що зловмисник використає усі можливі канали для здійснення неавторизованих дій. Для обчислення оцінки поверхні атак вважається, що зловмисник використає усі канали зв'язку у спробі здійснити атаку на автомобіль. Для усіх атак оцінка зусиль для доступу до каналів розраховується наступним чином:

$$E_c = E_{physical} + E_{short-range} + E_{long-range} = 16 \quad (2)$$

Оцінювання зусиль для доступу до даних. До даних, що представляють інтерес для зловмисника відносяться:

– формат даних, що використовує ЕКУ під час своєї роботи,
– зміст та дійсні значення кожного параметра,
– ключі для здійснення аутентифікації з ЕКУ,
– формат діагностичних команд.

Зловмисник отримує формат даних завдяки зчитуванню пакетів з CAN шини. Ці дані передаються в незашифрованому вигляді. Зміст та значення параметрів зловмисник отримує перебором усіх можливих значень (фазингом) та аналізуючи те, як змінюються значення. Оцінка зусиль для отримання таких даних встановлюється такою: $E_{plaintext} = 1$.

Дані можуть бути зашифровані, що вимагає знання ключа для розшифрування. В такому випадку зусилля для отримання доступу до даних мають наступну оцінку $E_{ciphertext} = 5$

Ключі для здійснення аутентифікації з ЕКУ та діагностичні команди не передаються під час нормальної роботи ЕКУ, тому

зловмиснику необхідно перебирати усі можливі комбінації. Оцінка зусиль для отримання доступу до даних складає $E_{hidden} = 10$.

Для оцінки зусиль для доступу до даних вважається, що зловмисник спробує отримати усі можливі дані, що допоможуть здійснити атаку [5].

Для усіх атак, де використовуються лише нормальні пакети, оцінка зусиль становить

$$E_d = E_{plaintext} = 1 \quad (3)$$

Для атак з використанням діагностичних команд зусилля оцінюються як

$$E_d = E_{hidden} = 1 \quad (4)$$

Оцінювання зусиль для доступу до методів. З точки зору атакуючого ЕКУ є чорним ящиком, що реагує на дані, що містяться в вхідному пакеті. Простішим способом здійснення атаки є надсилання пакетів, що з'являються в мережі, але з модифікованими значеннями. Далі буде використовуватися термін атака з використанням нормальних пакетів для подібних атак. Оцінка зусиль для доступу до методів в такому випадку складає $E_{unconditional} = 1$.

Деякі ЕКУ вимагають появи певних умов для виконання власних методів. Це може бути очікування зовнішньою події для іншого ЕКУ або спеціальні значення даних, якими ЕКУ володіє. Для виконання таких методів зловмиснику необхідно імітувати пакети від ЕКУ, результати якого очікує цільовий (атакований) компонент. Оцінка зусиль для доступу до методів складає $E_{conditional} = 5$.

Найбільші можливості для здійснення атаки відкривають діагностичні команди, оскільки вони дозволяють зробити те, що недоступно водію під час нормальної роботи. Проте атакуючому необхідно відкрити діагностичну сесію та дізнатися формат

діагностичних команд. Оцінка зусиль в такому разі складає $E_{diagnostic} = 10$.

Оцінка потенційних збитків. Для оцінювання потенційних збитків використовуються оцінки наслідків атак на ЕКУ автомобіля за методологією оцінювання загроз для автомобіля[8]. Наслідки здійснення атаки оцінюються за наступними критеріями[9]: безпека водія, експлуатаційні характеристики автомобіля, приватність даних, фінансові ризики, керованість ситуації. Використовуються результати атак здійснених дослідниками [3-5]. Результати оцінювання атак наведені в таблицях 1 та 2.

Таблиця 1

Значення оцінок строгості і керованості та загальної оцінки рівня атак під час звичайної роботи автомобіля

STRIDE	Безпека водія	Експлуатаційні характеристики	Приватність даних водія	Фінансові ризики	Керованість автомобіля	Оцінка загрози
1	**2**	**3**	**4**	**5**	**6**	**7**
Показ довільних значень на спідометрі						
S T	1	0	0	1	1	105
Показ довільних значень одометра (Форд)						
S T	0	0	0	2	0	10
Обмежена можливість керування (Форд)						
D	2	2	0	2	2	424
Показ довільних значень одометра (Форд)						
S T	0	0	0	2	0	10
Обмежена можливість керування (Форд)						
D	2	2	0	2	2	424
Показ довільних значень на спідометрі (Тойота)						
S T	1	0	0	1	1	105
Спрацювання гальм (Тойота)						
S T R	2	3	0	3	3	636
Керування автомобілем (Тойота)						
S T R D	3	3	0	3	3	936

Збільшення гучності радіо						
S T	1	0	0	0	1	100
Віддалений старт автомобіля						
S T	0	0	0	3	4	15
1	2	3	4	5	6	7
Вимикання двигуна						
S T R	4	3	0	3	3	1236
Визначення автомобіля						
I	0	0	3	0	0	15
Запис розмов в салоні автомобіля						
I E	0	0	3	0	0	15
Визначення положення автомобіля						
I E	0	0	3	0	0	15

Таблиця 2

Значення оцінок строгості і керованості та загальної оцінки рівня атак за допомогою діагностичних пакетів

STRIDE	Безпека водія	Експлуатаційні характеристики	Приватність даних водія	Фінансові ризики	Керованість автомобіля	Оцінка загрози
1	**2**	**3**	**4**	**5**	**6**	**7**
Спрацювання гальм (Форд)						
S T R	0	3	0	0	4	15
Блокування гальм (Форд)						
S T R	2	3	0	2	3	631
Вимкнення фар та освітлення (Форд)						
S T R	2	2	0	3	2	429
Вимикання двигуна (Форд)						
S T R	0	3	0	0	4	21
Вмикання/вимикання гудка (Тойота)						
S T R	1	0	0	0	3	300
Відкривання /замикання дверей (Тойота)						
S T R	2	2	0	3	2	429
Показ довільних значень на індикаторі палива (Тойота)						

S T R	2	1	0	3	2	422
Постійна активація реле блокування дверей						
R E	1	2	0	0	1	114
Безперервна робота склоочисників						
R E	1	0	0	0	1	100
Відкриття багажника						
S T E	0	0	0	3	3	15
Відміна блокування положення дросельної заслінки						
R E	2	2	0	0	2	400
Відкриття усіх дверей						
R E	1	2	0	3	2	229
Постійна робота гудка						
S R E	1	0	0	0	1	100
Вимикання усього допоміжного освітлення						
S R E	2	2	0	3	4	829
Безперервна подача рідини для склоочисників						
S R E	2	2	0	3	3	629
Тимчасовий приріст кількості обертів двигуна						
S R E	2	3	0	2	3	631
Вимикання циліндрів двигуна, рульового управління, гальм						
S R E	3	3	0	3	3	921
Збільшення кількості обертів двигуна в режимі спокою						
S R E	2	2	0	2	2	424
Спрацювання гальм для передніх колес						
S R E	3	4	0	4	4	1248
Розблокування гальм, запобігання гальмуванню						
S R E	4	4	0	4	4	1648

Дерево атаки. Дерево атаки [10] є зручним способом систематично класифікувати різні способи атакувати захищуваний об’єкт. В загальному вигляді атаки на об’єкт представляються в деревоподібній структурі, з ціллю атаки як кореневим вузлом та різними способами досягнення цієї мети як листи дерева. На рисунку 1 зображено дерево атаки, де кінцевою ціллю є відкриття сейфа.

Для того, щоб відкрити сейф зловмисник може використати відмички, дізнатися кодову комбінацію, розрізати сейф або скористатися тем, що сейф було встановлено з порушенням вимог. Комбінацію можна знайти записаною або дізнатися від власника і так далі. Кожен вузол, окрім кореневого, є підціллю, а всі підвузли є способами досягнення цієї проміжної цілі.

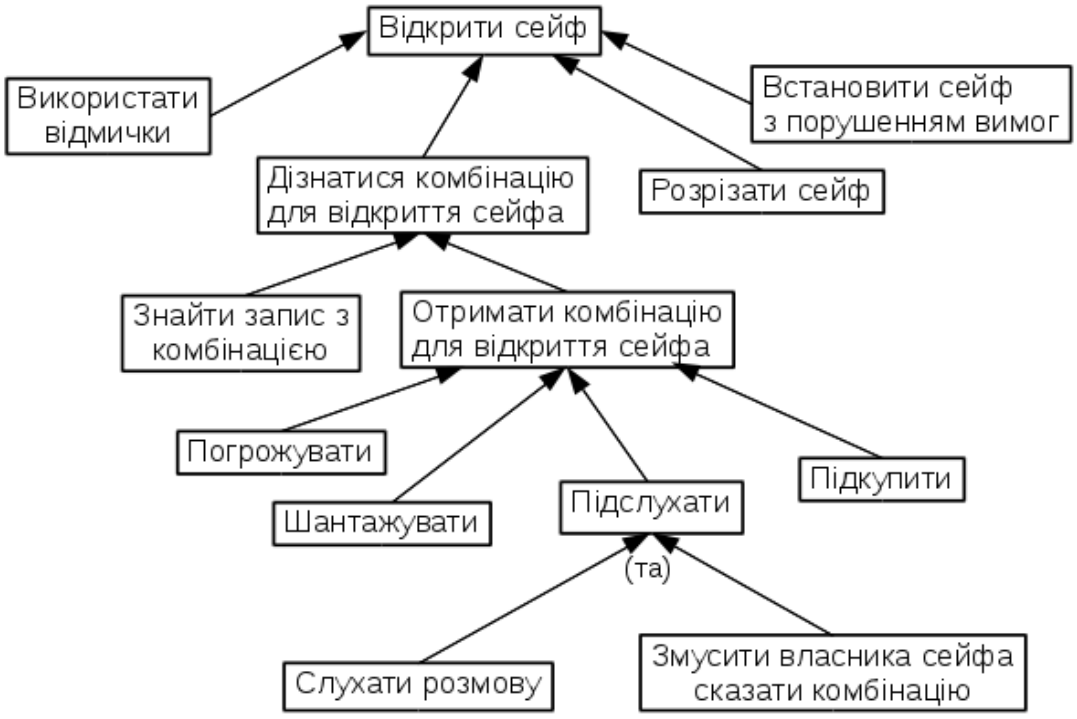

Рис. 1. Приклад дерева атаки на сейф.

Вузли можуть бути сполученими або альтернативними. На рисунку усі вузли, де не вказаний тип, є альтернативними вузлами. Сполучені вузли передбачають одночасне виконання умов усіх підвузлів, що можна порівняти з логічним “І”. Альтернативні вузли вимагають виконання хоча б однієї передумови, що є аналогією логічного “АБО”.

Наступним кроком є визначення для кожного вузла його значення. Наприклад, значення “Можливо” та “Неможливо”. Проте використання кількісних значень надає більше інформації та дозволяє оцінити ймовірність здійснення атаки. Кожен вузол в дереві атаки є

частиною її здійснення і вимагає певних зусиль для здійснення дії, що міститься в вузлі. Шлях від вузлів найнижчого рівня до кореневого визначає послідовність кроків зловмисника для здійснення атаки і сума зусиль кожного кроку можна розглядати як загальні зусилля зловмисника. Очевидно, що зловмисник буде витрачати мінімум зусиль, тобто пройде шляхом, сумарні зусилля якого будуть найменшими.

Варіанти здійснення атак. Атаки, описані в [3-5] направлені проти різноманітних ЕКУ в різних моделях автомобілів, проте аналіз цих атак дозволив виділити 2 основних алгоритми, за якими здійснювались ці атаки. Загальний алгоритм виконання будь-якої атаки на ЕКУ в CAN мережі зводиться до двох варіантів:

1) атака з використанням нормальних пакетів;
2) атака з використанням діагностичних команд.

На рисунках 2 та 3 зображені дерево атаки з використанням нормальних пакетів та дерево атаки з використанням діагностичних команд відповідно.

Приклади атак, що здійснюються за допомогою нормальних пакетів [3-5]:

- обмежена можливість керування через вплив на можливість повертати колеса,
- можливість віддаленого керування автомобілем (зміна напрямку руху),
- віддалений старт автомобіля.

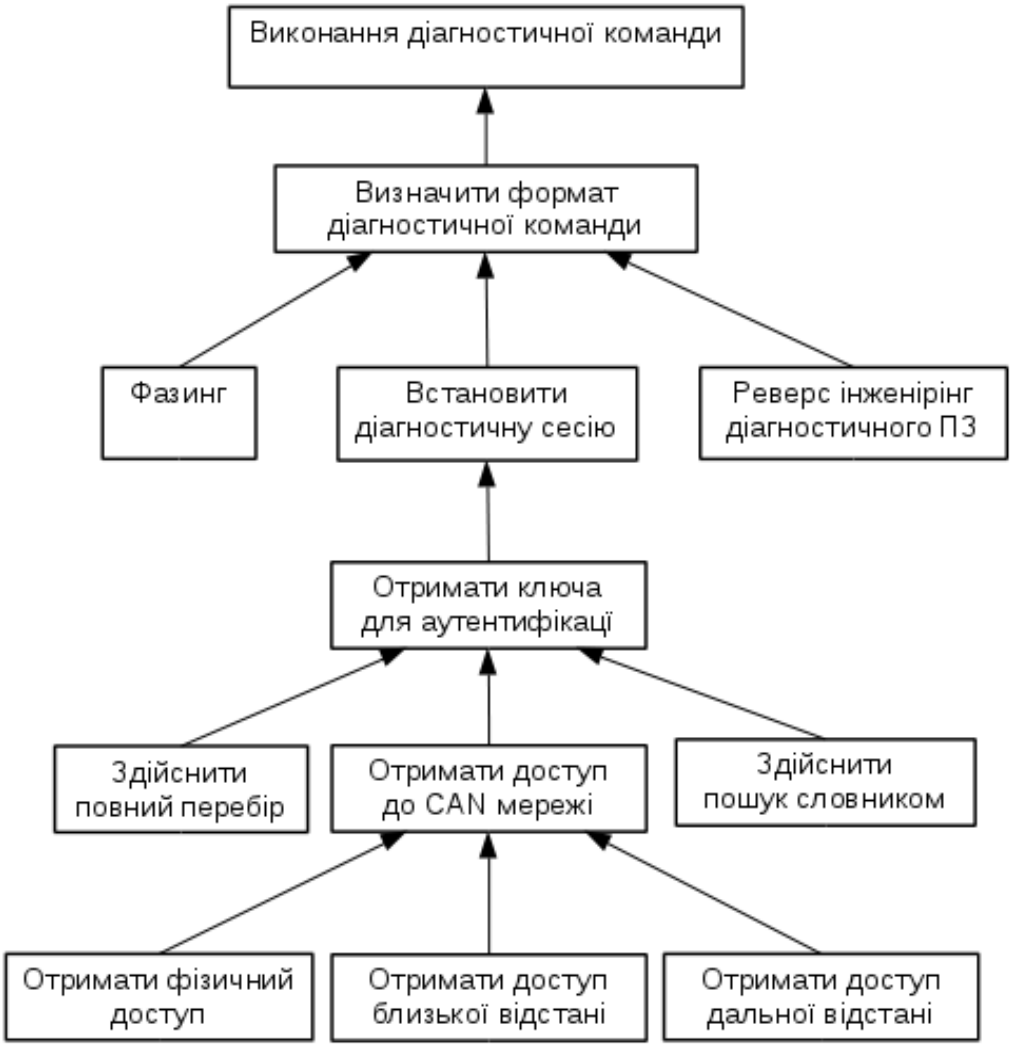

Рис. 2. Дерево атаки з використанням діагностичних команд

Кожна атака з використанням діагностичних команд передбачає розблокування ЕКУ, що є необхідним під час тестування виробником або представнику сервісного центру для здійснення діагностики автомобіля. Для розблокування необхідний криптографічний ключ для аутентифікації. Кожен ЕКУ має свій власний ключ, який не передається в відкритому вигляді.

Приклади атак з використанням діагностичних команд [3,5]:

- розблокування гальм, запобігання гальмуванню;
- вимикання двигуна;
- тимчасовий приріст кількості обертів двигуна;
- вимикання усього допоміжного освітлення;

– відкриття усіх дверей.

Рис. 3. Дерево атаки з використанням нормальних пакетів

На нижчому рівні в обох деревах (див. рисунки 2 та 3) знаходиться отримання доступу до мережі, що очевидно є першим кроком для здійснення будь-яких неавторизованих дій. Наступним спільним вузлом є визначення формату даних, який розпізнає ЕКУ, оскільки неправильно сформовані дані будуть відхилені. Можливість того, що ЕКУ не здійснює жодних перевірок дійсності вхідних можна вважати замалою.

Для визначення формату даних в обох випадках використовується техніка фазинг - техніка, яка полягає в тому, що на вхід програми подаються недійсні, невідповідні або випадково генеровані дані. В даному випадку метою є знаходження тих даних, які ЕКУ сприйме як дійсні.

Для здійснення атаки з використанням діагностичних функцій обов'язковою є відкриття діагностичної сесії, без якої неможливо змусити ЕКУ виконати будь-яку діагностичну функцію.

Одним з можливих кроків атаки з використанням нормальних пакетів є зміна прошивки нецільового ЕКУ. Це дозволить здійснювати атаку навіть без встановлення зв'язку з автомобілем, оскільки модифікований ЕКУ сам може здійснювати її, якщо настають певні події, що визначається цілями та мотивацією зловмисника.

Оцінка поверхні атак для ЕКУ модуль керування двигуном. Для переліку атак на ЕКУ модуль керування двигуном [3] отримані такі оцінки наслідків здійснення атак (див. таблицю 2 додатку):

- вимикання двигуна (T =1236);
- вимикання циліндрів двигуна, рульового управління, гальм (T = 921);
- тимчасовий приріст кількості обертів двигуна (T = 631);
- збільшення кількості обертів двигуна в режимі спокою (T =424).

Усі атаки здійснюються з використанням діагностичних пакетів, тому використовуються наступні значення зусиль:

$$E_c = 16, E_d = 10, E_m = 10 \quad (5)$$

Оцінка поверхні атак для модуля керування двигуном:

$$s_{ECM} = \frac{631 + 921 + 1236 + 424}{16 + 10 + 10} = 89.2 \quad (6)$$

Оцінка поверхні атак для ЕКУ модуль керування тілом. Згідно [3] перелік атак на ЕКУ модуль керування тілом (Body Control Module) та оцінки наслідків здійснення цих атак (див. таблицю 2 додатку) такі:

- вимикання усього допоміжного освітлення (T = 829);
- безперервна подача рідини для склоочисників (T = 629);
- відміна блокування положення дросельної заслінки (T = 400);

– відкриття усіх дверей (T = 229);
– постійна активація реле блокування дверей (T = 114);
– безперервна робота склоочисників (T = 100);
– постійна робота гудка (T = 100);
– відкриття багажника (T = 15).

Усі атаки здійснені з використанням діагностичних пакетів, тому використовуються значення зусиль ті ж самі, що і для попереднього ЕКУ.

Оцінка поверхні атак для модуля керування тілом:

$$S_{BCM} = \frac{114 + 100 + 15 + 400 + 229 + 100 + 829 + 629}{16 + 10 + 10} = 67.1 \quad (7)$$

Оцінка поверхні атак для ЕКУ модуль керування гальмами. Проведення атак на ЕКУ модуль керування гальмами (Electronic Brake Control Module) описано в [3]:

– розблокування гальм, запобігання гальмуванню (T = 1648);
– спрацювання гальм для передніх колес (T = 1248).

Оцінки наведені в таблиці 2 додатку. Атаки також здійснені з використанням діагностичних пакетів і оцінка поверхні атак складає:

$$S_{EBCM} = \frac{1248 + 1648}{16 + 10 + 10} = 80.4 \quad (8)$$

Оцінка поверхні атак з використанням нормальних пакетів. Атаки, що здійснюються лише надсиланням пакетів, які передаються під час роботи будь-якого ЕКУ вимагають від зловмисника лише доступу до мережі. Неможливо виділити конкретний ЕКУ для оцінки поверхні атак, оскільки будь-який ЕКУ в мережі є потенційною ціллю зловмисника, тому що він може надіслати через CAN шину пакет усім ЕКУ. Тому наводяться оцінки збитків усіх атак [3-5], що здійснюються з використанням нормальних пакетів.

– вимикання двигуна (T = 1236);

- керування автомобілем (T = 936);
- спрацювання гальм (T = 636);
- обмежена можливість керування (T = 424);
- показ довільних значень на спідометрі (T = 105);
- показ довільних значень на спідометрі (T = 105);
- збільшення гучності радіо (T = 100);
- віддалений старт автомобіля (T = 15);
- показ довільних значень одометра (T = 10).

Атакуючому потрібно докласти значно менше зусиль для здійснення цих

атак і тому загальна оцінка зусиль також є меншою, ніж для будь-якої атаки, пов'язаної з використанням діагностичних функцій:

$$E_c = 16, E_d = 1, E_m = 1 \quad (9)$$

Загальна оцінка для поверхні атак складає:

$$S_{normal} = \frac{105 + 10 + 424 + 105 + 636 + 936 + 100 + 15 + 1236}{16 + 1 + 1} = 198.16 \quad (10)$$

Отримана оцінка значно вища, ніж у будь-якої атаки з використанням діагностичних можливостей, що зумовлено значно меншими зусиллями і тим, що враховувались атаки на чисельні ЕКУ, а не один.

Висновки. Запропоновано підхід до кількісного оцінювання поверхні атак, який базується на використанні оцінок величин потенційних збитків від атак та оцінок зусиль для доступу до каналів, даних та методів ЕКУ. Використовуючи цей підхід отримані оцінки атак на ЕКУ, які відображають ступінь суворості наслідків атак. Так найбільші оцінки отримали ЕКУ модуль керування гальмами та ЕКУ модуль керування двигуном, що дійсно мають найгірші наслідки від зловмисних дій. Висока оцінка атак з використанням нормальних пакетів пояснюється відносною легкістю їх здійснення і значною

кількістю атак. Це зумовлено тим фактом, що зловмиснику достатньо отримати доступ до CAN мережі лише одним способом, щоб мати можливість атакувати усі ЕКУ в мережі. Кількісна оцінка поверхні атак дає змогу зрозуміти спеціалістам з інформаційної безпеки, які ЕКУ є найбільш привабливими для атакуючого з точки зору можливості здійснення атак. Також чим вище оцінка, тим більше векторів атаки, тобто способів здійснити неавторизовані дії.

References:

1. Attack Surface Analysis Cheat Sheet. Online: https://www.owasp.org/index.php/Attack_Surface_Analysis_Cheat_Sheet

2. Pratyusa K. Manadhata, "An Attack Surface Metric", November 2008.

3. K. Koscher et al., "Experimental security analysis of a modern automobile," in Proceedings — IEEE Symposium on Security and Privacy, 2010, pp. 447–462

4. Rouf, I. et al. Security and privacy vulnerabilities of in-car wireless networks: A tire pressure monitoring system case study. Proceedings of the 19th USENIX Security Symposium (2010).

5. Dr. Charlie Miller, Chris Valasek, "Adventures in Automotive Networks and Control Units". Online: http://illmatics.com/car_hacking.pdf.

6. S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, K. Koscher, A. Czeskis, F. Roesner, and T. Kohno, "Comprehensive experimental analyses of automotive attack surfaces". In Proceedings of the 20th USENIX Conference on Security, SEC'11.

7. AUTOSAR FO Release 1.3.0 Glossary. Online: https://www.autosar.org/fileadmin/user_upload/standards/foundation/1-3/AUTOSAR_TR_Glossary.pdf

8. Stijn van Winsen, “Threat Modelling for Future Vehicles, On Identifying and Analysing Threats for Future Autonomous and Connected Vehicles”, 2017.

9. David Ward, Ireri Ibara, and Alastair Ruddle. “Threat Analysis and Risk Assessment in Automotive Cyber Security.” In: SAE International Journal of Passenger Cars-Electronic and Electrical Systems 6.2 (2013), pp. 507–513. issn: 1946-4622. doi: doi:10.4271/2013-01-1415.

10. Mauw, S., Oostdijk, M.: Foundations of Attack Trees. In Won, D., Kim, S., eds.: ICISC. Volume 3935 of LNCS., Springer (2005) 186–198.