УДК 681.3.06:519.248.681 **DOI:10.30837/rt.2020.4.203.09**

І.Д. ГОРБЕНКО, д-р техн. наук, Д.О. ФЕСЕНКО

ВИКОРИСТАННЯ BLOCKCHAIN В АВТОМОБІЛЬНІЙ БЕЗПЕЦІ (AUTOMOTIVE SECURITY)

Вступ

Сучасними системами захисту автомобілів все більше цікавляться зловмисники, автомобілі стають більш технологічними, це в свою чергу відкриває нові можливості компрометації роботи вузлів та систем автомобіля, тому до систем безпеки пред'являються все більш жорсткі вимоги щодо забезпечення ефективності та безпечності їх функціонування. Сучасні системи захисту від незаконного заволодіння автотранспортом, більш відомі як «сигналізація», намагаються стримувати атаки зловмисників, але в свою чергу можуть привносити додаткові бекдори для зловмисників зовсім ненавмисно, наприклад додаючи цікаву функцію в систему автомобіля, а згодом ця функція може мати двояке значення через проблеми з системою автентифікації. Тож, системи безпеки автомобіля повинні мати найвищий рівень безпеки автентифікації, для реалізації якого пропонується використання децентралізованої мережі блокчейн з вузлами для кожного автомобіля, що автентифікують користувача групово, це дозволить відійти від стандартної клієнт-серверної архітектури, що є недостатньо захищеною. Основними шляхами вирішення зазначеної проблеми є побудування комплексної системи безпеки, що, в свою чергу, включає покращений та надійний захід автентифікації на основі децентралізованої мережі блокчейн та двох комплексних схем оновлення системи передачі критичних даних автомобіля – мережі CAN. Використання даних систем дозволить поліпшити показники захищеності системи автентифікації та інформації, що курсує між блоками критичної важливості, що покращить безпечність автомобіля як від угонів, так і від можливостей створення зловмисниками аварійних ситуацій дистанційно.

Мета статті – розгляд існуючих систем автентифікації для системи безпеки автомобіля та можливостей з інтеграції децентралізованих технологій для систем безпеки автомобіля на прикладі системи автентифікації.

1. Дослідження проблем сучасних автомобільних систем безпеки

Зараз існує багато брендів, що випускають продукцію для захисту безпеки автомобілів за допомогою різноманітних видів сигналізації. В описах своїх продуктів вони пропонують дуже гарну захищеність майже від всіх атак, але чи насправді це так? Цікавим є те, що всі розробки побудовані на добре відомій клієнт-серверній архітектурі.

Розглянемо дослідження різних команд, що займаються проблемами безпеки транспортних засобів, які були оприлюднені за результатами тестування безпечності найбільш використовуваних систем сигналізації.

Першою системою є рішення, при детальному розгляді якого виявилося, що в бекенд частині системи безпеки є небезпечні прямі посилання, що знаходяться прямо в головному API, тобто, використовуючи спеціально підготовлені параметри, можна без авторизації змінити критичні дані користувача, обновити пароль для доступу до акаунту та усі пов’язані з цим дані. Таким чином, зловмисник повністю отримує доступ до системи безпеки автомобіля, може додати свій ключ доступу до автомобіля. Повну процедуру розглянемо далі. Керування автоматичною трансмісією складається з кількох підсистем, що взаємопов’язані між собою та виконують свої функції, що в сукупності і дозволяє компонентам системи синхронізовано та правильно між собою працювати.

Підсистема обробки інформації забезпечує створення, зберігання, актуалізацію інформації про стан блоків транспортного засобу та можливості керування ними і складається із засобів обробки інформації, системного та функціонального ПЗ.

До засобів обробки інформації належать бортовий комп'ютер та встановлена кількість блоків керування для забезпечення всіх функцій щодо роботи, супроводження транспортного засобу та захисту інформації. Підсистема взаємодії з користувачами АС забезпечує моніторинг, керування даними блоків транспортного засобу, з використанням мереж передачі даних та стандартних CAN та LIN-протоколів.

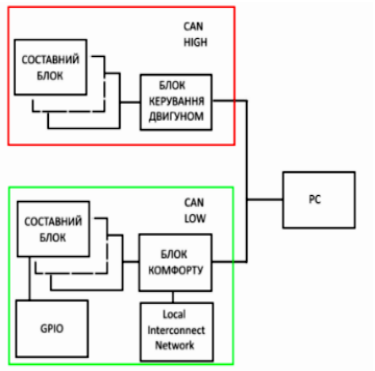

Рис. 1. Склад робочої станції

Технічні засоби, що встановлені на даному транспортному засобі та цікавлять нас при проведенні даного типу огляду, взаємопов'язані в мережу CAN, або контактують з нею.

Мережа CAN ділиться на два рівні абстракції: CAN High, в колі якого взаємодіють надзвичайно важливі для правильної роботи механізмів транспортного засобу блоки. Наприклад, в блок керування двигуном можна було б відправляти заготовлені зловмисником повідомлення для атаки інших блоків. Розглянемо приклади таких атак.

Перший вид атак – атаки на мережі, які підтримуються даним транспортним засобом, – це мережа Bluetooth, вектор атаки якого використовує помилки реалізації протоколу та дозволяє виконати атаку спарювання пристрою атакуючого з пристроєм, встановленим на авто.

Інший напрям – це мережа Wi-Fi, яка найчастіше буде використовуватися для доступу до мережі інтернет з метою серфінга інтернет-сторінок, оновлення навігаційних карт. Тут атаки можуть бути різноманітні: від реалізації атаки на стек до можливостей проведення Fake AP/MITM атаки.

В авто також встановлена система навігації GPS – ще один можливий напрям атаки, який, наприклад, може реалізовувати спуфінг координат або ж використовувати атаку на реалізацію самої системи.

Кожен автовиробник використовує спеціальну протиугонну систему – імобілайзер, що встановлюється в електронну систему керування та блокує роботу двигуна, якщо не знайдено спеціального ідентифікатора, що знаходиться в ключі автомобіля. Основна проблема в тому, що штатний імобілайзер не дозволяє підключень інших пристроїв до себе і подальшого їх використання. Для керування системами двигуна з використанням сторонніх систем безпеки виробники цих систем пропонують пристрої обходу імобілайзеру, що несе ще більше загроз. Розглянемо їх детальніше. Під час розгляду іншою командою дослідників було знайдено вразливість, яка використовує атаку на саме таку систему обходу імобілайзера. Як було вказано, система імобілайзеру повинна блокувати роботу двигуна і у випадку, коли був використаний варіант з обходу штатного імобілайзера, відкривалась можливість керувати системою імобілайзера через інтерфейси системи безпеки. Це з боку виробника подається в якості додаткової системи захисту, що начебто дозволить зупинити машину, якщо її вкрали і переганяють, але чином вся система через одну вразливість в серверній частині дозволяє зловмиснику зупинити двигун, коли це потрібно, що може привести до трагічних наслідків. Також виробники систем захисту використовують мережу CAN(Controller Area Network) для інтеграції своїх систем, що спрощує встановлення такої системи в авто, оскільки, використовуючи цю мережу, система безпеки може самостійно визначити дані про транспортний засіб

та на основі цих даних налаштувати систему та ввести її в дію. Але і в цьому плюсі є великий мінус: частіше за все пристрій системи безпеки доданий до мережі у гілку важливих частин автомобільних систем і таким чином скомпрометований пристрій може керувати іншими пристроями, пов'язаними з цими мережами таким самим чином, що і дозволяє системі безпеки отримувати дані про автомобільні системи. Цей канал зв'язку можна назвати дуплексним, він дозволяє як читати дані, так і записувати, тобто передавати команди пристроям, що знаходяться на одному рівні з системою безпеки. Пристрої – це електронні блоки, що керують важливими електронними системами автомобіля, а які саме – залежить від того, де встановлена скомпрометована система безпеки. Через відсутність автентифікації в протоколі CAN стає можливим маскувати ECU або замінити легальний ECU зловмисним за допомогою апаратного пристрою. До CAN-шини також може бути приєднаний пристрій зловмисника, який може не завжди спеціально представляти собою закладний пристрій, а може бути пристрій, який просто має в собі вразливості через їх недостатню захищеність, або й встановлений саме зловмисниками, наприклад під час ремонтних робіт, оскільки мережеві дроти більшості транспортних засобів легко виявити та використовувати для з'єднання.

Розглянемо два сценарії нападу, які використовують підмінні повідомлення на CAN-шині. Перший сценарій ілюструє атаку, коли оригінальна програма ECU замінюється шкідливою. Другий сценарій являє собою атаку, коли неавторизований пристрій підключено до CAN-шини. За безпеку в мережах та інформації в ЄС відповідає Агентство Європейського Союзу з питань мережевої та інформаційної безпеки (ENISA), воно має сприяти та захищати передові практики щодо безпеки та стійкість критичного систем. Останнім часом агентство опублікувало звіт, в якому описує відсутність безпеки в поточних мережах автомобілів і представляє ряд можливих загроз і моделей нападу, які можуть бути виконані в мережі для виявлення стану кібербезпеки та стійкості систем автомобілів. Серед іншого, у доповіді згадується, що атака типу man-in-the-middle можлива шляхом підключення несанкціонованого пристрою безпосередньо до шини CAN. Також у звіті зазначено, що атаки відтворення дозволяють зловмисникам виявляти команди, які контролюють критичні системи безпеки, а також вказує на вразливість до атак відмови в обслуговуванні. Сучасні автомобілі мають спеціальний діагностичний порт, який називається портом OBD-II (бортовий діагностичний пристрій), який знаходиться під приладовою панеллю автомобіля. Цей інтерфейс дозволяє технікам виконувати діагностику засобів в мережі, перевіряти контроль викидів і повідомляти про будь-які несправності. Реалізація цього порту в автомобілях стала обов'язковою як у США з 1996 р. і в ЄС з 2001 р. Відомо, що за результатами дослідження, що були проведені незалежними експертами щодо автомобільної безпеки деяких автомобілів, є можливість ввести підроблені повідомлення на CAN шину Toyota Prius та Ford Escape. Ця атака була успішно проведена через те, що протокол CAN не надає жодної форми автентифікації, а повідомлення передаються по всій мережі у режимі широкомовної передачі. Опублікований звіт містить докладний опис того, як було здійснено атаку і на яких машинах було проведено атаку. Звіт також включає в себе архітектуру CAN, реалізовану в обох автомобілях, і їхні відповідні схеми підключення, код, який використовується для виконання атаки, і ідентифікатори повідомлень CAN обох автомобілів разом з відповідними функціями. Налаштування цієї атаки складалося з ноутбука, підключеного до порту OBD-II. Через те, що вдалося прочитати та записати в CAN-шину дані, ідентифікатори повідомлень були успішно ідентифіковані та була успішно виконана атака відтворення. Результати цього експерименту показали, що можливо відправляти підроблені повідомлення до важливих блоків для обох розглянутих в доповіді транспортних засобів, що призвело до відключення або примусового застосування гальм, вимкнення двигуна, відображення підроблених значень на панелі приладів, блокування та розблокування дверей і втручання як в внутрішні, так і в зовнішні вогні. В загальному вигляді пристрій, навіть якщо він не скомпрометований, буде підключений, тому для мережі при правильному налаштуванні компрометуючого пристрою (вірно проставлених ідентифікаторів пристрою та інше) буде виглядати як нескомпрометований пристрій, що готовий до робо-

ти. У випадку компрометації пристрою атака буде виконана в декілька етапів. По перше, треба вибрати пристрій для компрометації, наприклад розглянемо як такий пристрій ECU2, що є яким-небудь легкодоступним пристроєм, визначимо, що ECU2 буде видавати себе за пристрій ECU4, який буде пов'язаний з ECU двигуна. Для того щоб ECU2(NEW ECU4) став повністю працюючим скомпрометованим пристроєм, необхідно щоб пристрій не був дублікатом, тому його необхідно вимкнути. Для того щоб вимкнути пристрій з мережі, можна використати DOS атаку. Данні атаки мають багато варіантів реалізації, розглянемо деякі з них: DoS всієї шини дозволяє повністю запобігти комунікації CAN, генеруючи в шині безперервні з'єднання; цей стан не дозволить будь-якому вузлу надсилати повідомлення. Для проведення атаки необхідно згенерувати постійний рівень «0» в лінії приймача CAN. Багато реалізацій CAN мають вбудовані механізми запобігання таким порушенням. Але цей варіант не підходить для даного виду атаки, оскільки так вся мережа стане недоступною. Направлена DoS атака «DoS ACK» може бути направлена на один пристрій в мережі, вводячи домінуючі біти тільки в повідомленнях, надісланих на цільовий вузол. Для цього атакуючий повинен мати точні дані про ідентифікатори повідомлень, відправлених певним вузлом. Контролюючи шину для цільових ідентифікаторів, вона повинна вводити необхідні біти після фази арбітражу. Така заміна призводять до втрати цільових даних, лічильник помилок зростає, мережа відкидає пристрій з пріоритетності передачі і, тим самим, пристрій можна вважати вимкненим. Цей варіант повністю підходить для даного виду атаки, оскільки в цьому випадку стає недоступним лише пристрій, що атакується, а вся мережа працює в звичайному режимі. Після компрометації блоку відкривається можливість для проведення атак від імені скомпрометованого блоку. Шина CAN має послідовну схему з'єднання, тобто біти передаються один за одним від старшого біта до молодшого. Поняття байт до CAN зазвичай не вживається, тому в основному оперують терміном «поле». Довжина поля не повинна бути кратна байту (8 бітам). Протокол обміну даними проводиться фреймами. Фрейм складається з чотирьох основних полів: кода відправника, він же є основою арбітражу передачі даних; керуючого поле; даних; контрольної суми. Особливістю цього інтерфейсу є те, що біт, який передається, приймається приймачем CAN. Це допомагає проконтролювати правильність передачі даних та вести арбітраж на лінії між бажаючими передати дані. Передача йде «зліва направо», тобто першим піде ідентифікатор. При передачі ідентифікатора вузол вивчає стан лінії. Якщо необхідно передати 1, а на лінії раптом опинився 0, то це буде означати, що який-небудь більш пріоритетний ECU намагається передати свої дані. У цій ситуації передавач, який впіймав 0 замість переданого 1, не передає дані. Таким чином, чим менший ідентифікатор у передавального вузла, тим вище у нього пріоритет. Оскільки сучасний автомобіль практично всім керує за допомогою контролерів, тому і необхідно захищати з'єднання між блоками. Для цього необхідно розглянути декілька видів архітектури, що дозволила б надійно контролювати цілісність та відповідність даних, що передаються.

2. Захищеність мережі блокчейн

Багато відомих брендів автовиробників хочуть встановлювати на свої автомобілі власні системи безпеки з різними ідентифікаторами доступу для ідентифікації користувачів з їх транспортними засобами, але все одно всі ці сучасні розробки використовують систему з центральним сервером, який обробляє все запити. Розглянемо детальніше можливі сценарії, що можуть трапитися через такі вразливості. В системі такого типу встановлюється система глобального позиціювання, що відправляє на сервер дані про місце розташування автомобіля, тобто, отримавши доступ до аканту користувача, зловмисник може легко дізнатися, де знаходиться автомобіль, та вкрасти його, не докладаючи великих зусиль на пошук чи відстеження автомобіля. Якщо розглядати даний випадок з можливістю зміни чи отримання будь-яких даних, то будь-який більш-менш досвідчений розробник програмного забезпечення може зробити парсер для пошуку в базі автомобілів за маркою, роком випуску, місцем знаходження та іншими визначними параметрами, що зберігаються в акаунтах користувачів, та

можуть надаватися іншим зловмисникам за плату з метою знаходження бажаного автомобіля під замовлення. Це робить систему з централізованим доступом зберігання даних дуже небезпечним. Останнім часом з'являються нові проекти на основі децентралізованої системи блокчейн, що дозволяє вирішити питання автентифікації найбільш ефективно. Блокчейн – це система регістрів, які являють собою розподілену систему та не мають центрального органу, що складається з реєстрів обліку криптографічно підписаних транзакцій, згрупованих в блоки, де кожен блок пов'язується з попереднім після перевірки. На базовому рівні вони дозволяють спільноті користувачів записувати транзакції в загальнодоступному реєстрі групи користувачів цієї системи таким чином, щоб ніяка транзакція не могла би бути змінена після опублікування. Завдяки цим можливостям блокчейн успішно використовується для розробки рішень для різних сфер застосування, в першу чергу – в сфері електронної валюти. Після додавання нових блоків попередні блоки все важче модифікувати, оскільки вони копіюються по всіх реєстрах обліку всередині мережі та будь-які конфлікти вирішуються автоматично за допомогою встановлених правил.

Розглянемо можливі атаки, що можуть бути проведені для отримання неправомірного доступу до автомобілю зловмисниками. Ці атаки витікають з загальновідомих атак на будь-яку систему, що використовує в собі мережу блокчейн:

1) Атака Сібілли – тип атаки, що можливий в однорангових мережах, в яких вузол в мережі працює одночасно з декількома ідентичностями і підриває авторитет/владу в репутаційних системах. Основна мета цієї атаки – отримати більшість впливу в мережі для здійснення незаконних (стосовно правил і законів, встановлених у мережі) дій у системі;

2) DDoS (Distributed Denial of Service) – тип атак, ідея якої полягає в пересиланні великої кількості схожих запитів на один конкретний сервер або цілу мережу серверів з метою виходу з ладу частини мережі;

3) Зламування криптоалгоритмів. Злам алгоритмів, що використовуються для криптографічного захисту даних, що передаються та зберігаються, наприклад обчислення гешфункцій SHA-256 і ECDSA, вважаються досить стійкими при існуючих обчислювальних потужностях. Однак поява високопродуктивних квантових комп'ютерів збільшить ризик злому цих криптографічних функцій.

4) Пошук помилок та «бекдорів» у коді протоколів. На сьогодні це найбільша загроза для проектів, що будуються на базі блокчейн. Оскільки ця сфера є досить новою та складною навіть для досвідчених розробників, то час від часу знаходяться нові помилки у коді, що можуть завдати суттєвої шкоди усій системі;

5) (MITM) – атака типу людина посередині, це атака, яка більш за все нас цікавить при проектуванні системи безпеки автомобіля. В загальному випадку розглянемо в ролі вузлу, що буде атакуватися «Вузол 1», якому ми привласнимо ім'я Аліси (А), вузлу, що буде працювати з Алісою («Вузол 2») привласнимо ім'я Боб (В), також маємо зловмисника, який поставив собі за мету скомпрометувати, якого будемо називати Мелорі (Е).

Аліса відправляє Бобу повідомлення про запит на отримання блоку для синхронізації, яке перехоплює Мелорі:

$$A \overset{E}{\nrightarrow} B : \text{BLOCK REQ}$$

Розглянемо випадок, коли не буде використовуватися шифрування, а лише гешування блоків в вузлах, таким чином, не потрібно отримувати ключі шифрування.

Мелорі передає повідомлення Бобу, Боб на даному етапі не розуміє, що це повідомлення не від Аліси:

$$E \rightarrow B : \text{mod data}$$

Мелорі перехоплює блок Боба та модифікує його:

$$A \overset{E}{\nleftarrow} B : \text{BLOCK DATA}$$

Мелорі відправляє Алісі модифікований блок:

$$A \leftarrow E : \text{MOD BLOCK}$$

Аліса, отримавши повідомлення, намагається додати дані до ланцюгу блоків, але через використання механізму зберігання попередніх блоків виявляється факт підміни геш-значення пов'язаного блоку, і атака стає неможливою, а якщо цей блок ще не фігурував в блокчейні, то ця атака можлива. Для унеможливлення цієї атаки необхідно використовувати захищене з'єднання, що використовується далеко не завжди.

Ці атаки стають неможливими через те, що платформа, що планується до використання, вже має достатню кількість користувачів та надійне зберігання даних, що підтверджене роками використання платформи iOS, яка постійно оновлюється. Ця децентралізована система підходить для створення системи безпеки автомобіля наступного покоління, що забезпечила б гарний рівень гарантії для автентифікації користувачів.

Розглянувши детальніше принципи побудування системи на основі такої технології та потенційні атаки, можна зрозуміти, що рівень гарантій буде залежати від наявності достатньої кількості учасників. Будувати систему самостійно не є правильним рішенням. Необхідно використовувати платформи, в яких все достатньо користувачів та розповсюдженість буде найбільша.

3. Прототип системи CARKEY для автентифікації за допомогою мобільних пристроїв

Електронні коді доступу ключів CarKey зберігаються у додатку Wallet на iPhone користувача, функція CarKey нещодавно з'явилася у iOS 13.4. Спільний доступ до CarKey з кимось дозволить цій особі використовувати свій iPhone або Apple Watch для доступу до автомобіля, тримаючи пристрій біля зчитувача NFC, розташованого всередині транспортного засобу. Ключі можуть бути постійними (для подружжя) або тимчасовими (для водія або механіка). Функція CarKey дозволяє використовувати ваші iPhone та Apple Watch для розблокування/блокування автомобіля, запуску двигуна та керування автомобілем. Доступ до CarKey також як до Apple Pay та Apple Cash, засвідчується біометрично, використовуючи Face ID або Touch ID, щоб переконатися, що особа, яка тримає iPhone, є особою, яка має дозвіл на доступ до автомобіля.

Apple буде співпрацювати з виробниками автомобілів для CarKey, що вказує на те, що це може бути заводський варіант, подібний до CarPlay. CarKey вимагає транспортного засобу з NFC, тому виробники транспортних засобів повинні реалізовувати так, як це було «CarPlay» – мультимедійна система для автомобілів, що була розроблена Apple та активно використовується в даний час.

Apple є членом консорціуму автомобільної зв'язку (CCC), який розробив специфікацію Digital Key 2.0 на базі NFC, яка була доступна наприкінці 2019 року. Нова специфікація встановлює безпечний зв'язок між мобільними пристроями та транспортними засобами через NFC.

Консорціум CCC також працює над специфікацією Digital Key 3.0, заснованою на Bluetooth Le та Ultra Wideband, що дозволяє пасивний доступ до безключового ключа. IPhone 11, 11 Pro та 11 Pro Max від Apple підтримують ультраширокополосний діапазон, тому це функція CarKey, яку ми могли б побачити в майбутньому. Можливості отриманого програмно-апаратного комплексу із застосуванням додаткового відповідного математичного апарату дозволяють здійснювати синтез та аналіз безлічі класів сигналів, у тому числі й тих, які наведено у даній публікації.

4. Вразливості системи передачі даних NFC

NFC працює на дистанції до 10 см на частоті 13,56 МГц. Технологія потребує обов'язкової наявності відправника і отримувача. Пристрій відправника генерує активне поле, а пристрій отримувача зчитує його в пасивному режимі. Цікавим для зловмисників є

можливість отримання доступу до даних, що передаються по каналу передачі даних NFC, та методи захисту від такого виду атак. Над цими питаннями вже працюють вчені та хакери з усього світу, та вже є деякі успіхи в цьому, дослідникам вдалося отримати дані тестових NFC-приладів, що перебували на відстані 45 см від одержувача інформації. Відомий також вірус, що використовував relay-атаку та був створений з метою атакувати операційні системи смартфонів, що ініціював використання NFC смартфоном, що в свою чергу надсилав дані банківської карти зловмисникам, які, в свою чергу оплачували покупку карткою, використовуючи ретрансльовану транзакцію. Ще однією атакою на мережу NFC можна вважати використання засобами радіоелектронної боротьби або RFID-джаммерів. При їх використанні порушується робота ініціатора відправлення і система перестає працювати.

Розглянемо захист від атак на мережі, що використовують NFC. Безконтактна технологія, зручна, але як і кожна система має вразливі місця. Щоб забезпечити передачу даних NFC, при проектуванні системи важливо врахувати ризики, що пов'язані з можливістю елевації прав суперкористувача сторонніми додатками на смартфоні, якщо пристрій підтримує Root-доступ. Бажано налаштування, при якому система з Root-доступом на пристрої не буде працювати, або в такому випадку буде додатково використаний рівень абстракції з надійним шифруванням, оскільки отримання елевації прав дозволить з більшою вірогідністю встановити зловмисне програмне забезпечення.

Розглянемо втрату або крадіжку смартфону, на якому не встановлене блокування по пінкоду або відбитку пальця, та що зберігає NFC ідентифікатор.

5. Вибір платформи для зберігання ідентифікатору користувача

Компанія Apple на світовому ринку досить довгий час та продала вже приблизно два мільярди тільки лише iPhone, таким чином, використовувати таку платформу для цієї розробки дуже ефективно. Схема використання технології CarPlay є використання цієї платформи як основи для проміжного слою для інтеграції блокчейн-автентифікації, в якій CarPlay буде виконувати функції зв’язку з автомобілем та зберігання проміжних даних у захищеному сховищі, що в архітектурі Apple відомо як Wallet. На початковому етапі для використання системи користувачу необхідно завантажити додаток з офіційного магазину Apple – AppStore, що й буде основою керування доступу до автомобіля. Додаток являє собою повноправний вузол мережі блокчейн, що буде використовувати для зберігання критичних даних пристрій користувача. Після реєстрації, виконання усіх налаштувань та тестування роботи налаштувань пристрій буде доданий до мережі блокчейн та буде використовуватися для захисту автомобіля. В специфікаціях CarKey вказано, що є можливість передачі повноважень з доступу до автомобілю іншим особам. В рамках цієї блокчейн системи для цих цілей за необхідності будуть видані тимчасові токени для доступу стороннім особам. Для автентифікації в додатку необхідно буде вибрати дію, яку необхідно виконати з автомобілем (відкрити/закрити, дозволити запуск двигуна, чи інші дії, що доступні в залежності від встановленої комплектації засобів захисту), також, при наявності смарт-годинника Apple Watch буде можливість використовувати його як мітку для автентифікації, доступ до додатку також буде доступний з екрану Apple Watch. Після створення запиту на виконання дії з транспортним засобом він буде направлений до мережі блокчейн, де інші вузли повинні підтвердити, що пристрій та користувач, що створив запит є саме тим, кого за себе видає, все це проходить в автоматизованому режимі, підтвердження проходить за рахунок пристроїв, які мають запущеними додаток (навіть як сплячий процес). Після успішного підтвердження користувача надається доступ до можливості генерування мітки доступу для автентифікації. Якщо ви використовуєте Apple Watch, ви знаєте, що він пов’язаний з вашим iPhone (принаймні більшу частину часу). Він має доступ до більшості даних, які є на вашому iPhone – до ваших контактів, календарів, електронних листів, повідомлень тощо. Хоча Apple Watch підключається до iPhone з використанням систем автентифікації, все ж є ймовірність, що якщо ваш годинник загублений або вкрадений, хтось може отримати доступ до деяких ваших особистих даних. Додаток Watch

на iPhone дозволяє налаштувати багато налаштувань пристрою, і ви можете отримати доступ до деяких із них через додаток «Налаштування» самого годинника, де ви можете налаштувати параметри розблокування Apple Watch за допомогою iPhone, що робить Apple Watch доступним до використання, поки годинник знаходиться на зап'ясті. Ви можете налаштувати це налаштування в налаштуваннях пароля програми Watch. Якщо вимкнути це налаштування, то вам доведеться вводити пароль кожного разу, коли ви кладете годинник. За замовчуванням Apple Watch просить встановити чотиризначний пароль. Це й є основою автентифікації користувача. Як і в iPhone, існує налаштування самоочищення даних, яке видаляє всі користувацькі дані на Apple Watch при спробах брутфорсу пін-коду годинника. Зловмисник, що заволодіє годинником, але не вгадає пароль після десяти спроб, ніколи не отримає ваші дані.

6. Загрози iOs. Джейлбрейк. Програмні атаки на NFC

Деякі загрози безпеки можуть йти від самого користувача. Наприклад, не кожного власника брендових гаджетів задовольняє обмежена можливість оновлення програмного забезпечення і встановлення лише схвалених і перевірених розробником додатків. Такі користувачі роблять джелбрейк (jailbreak) – процедуру отримання повного доступу до файлової системи iOS, яка можлива завдяки наявності вразливостей в системі безпеки операційної системи. Після проведених маніпуляцій разом з можливістю встановлення сторонніх додатків зростає ймовірність проникнення шкідливих програм.

Джейлбрейк (від англ. Jailbreak – «Втеча з в'язниці») – це організація несанкціонованого розробником доступу до файлової системи в iOS з метою відкрити перед користувачем можливість установки додатків з неофіційних репозиторіїв і дослідження внутрішнього середовища ОС. Як правило, для цього використовуються виявлені в iOS вразливості. Саме тому можливість джейлбрейку з'являється зазвичай дещо пізніше виходу чергової версії iOS. Apple згодом закриває виявлені вразливості, але дослідники відшукують все нові і нові лазівки. На даний момент методи встановлення джейлбрейку прийнято ділити на дві умовні категорії.

Відв'язаний (неприв'язаний) джейлбрейк (untethered jailbreak) робиться один раз і назавжди, такий пристрій можна перезавантажувати без втрати доступу до файлової системи. Злітає він тільки після перепрошивки пристрою. Очевидно, що подібний джейлбрейк можливий далеко не на всіх версіях iOS.

Полувідв’язаний джейлбрейк (semi-untethered jail-break) працює лише до першого перезавантаження або відключення живлення пристрою. Після включення айфона потрібно заново запустити утиліту джейлбрейка, яка повторно заллє на телефон всі необхідні компоненти і змусить його завантажитися в робочому режимі.

Після виконання операції джейлбрейку на пристрій буде встановлений спеціальний магазин додатків “Cydia”. З цього магазину додатків можна встановити додаткове програмне забезпечення для модифікації системи, також інші магазини з програмним забезпеченням, за допомогою яких, використовуючи сертифікати корпоративних розробників, вони встановлюють на пристрій будь-якого користувача свій контент. Додатки підписуються як «корпоративні розробники», причому на одному такому акаунті можуть перебувати відразу декілька «магазинів». Корпоративний профіль купується в мережі і сфабрикувати необхідний не так вже й складно.

При завантаженні будь-якої програми з App Store на iPhone або iPad з'являється .ipa файл, який підписується вашим обліковим записом, щоб його не можна було запустити на іншому пристрої (наприклад, щоб ви після покупки гри не могли «передати» її одному безкоштовно). Сторонні «магазини» роблять те саме, підписуючи файли під своїм обліковим записом. Але щоб ці програми можна було встановити, на iPhone або iPad необхідно встановити спеціальний профіль, який підтвердить, що на вашому пристрої можна використовувати дані .ipa файли. Власне, користувачі роблять це самі. Після цього вони, задоволені, біжать

завантажувати безкоштовні програми на свої iPhone і iPad (або додаток зі зламаними вбудованими покупками). І дуже сильно ризикують.

Але деякі додатки можуть містити в собі зловмисний код, оскільки додатки в таких магазинах не перевіряють, як це робиться в офіційному магазині «App Store» від Apple.

Власники подібних «магазинів» можуть виявитися шахраями (в більшості випадків так воно і є), які залучають користувачів безкоштовними додатками. Самі вони поширюють програми, що містять шкідливий код, або, що ще гірше, інструменти для отримання доступу до даних на пристрої. Оскільки вони працюють безпосередньо з файлами додатків, звичайна гра може виявитися, наприклад, прихованою програмою.

При запуску додатків, створених за допомогою модифікованої версії Xcode, пристрій відправляв зловмисникам пакет даних про користувача. У нього входили назва програми, час, тип і унікальний ідентифікатор пристрою, країна місця знаходження та мова інтерфейсу, а також тип підключення до інтернету.

Крім цього, XcodeGhost відображав підроблені повідомлення від додатків (наприклад, щоб через фішингові схеми змусити користувача ввести свої дані), перехоплював процес відкриття сторонніх посилань, а також міг читати вміст буфера обміну системи. Останнє дозволяло зловмисникам красти паролі користувачів, скопійовані з сторонніх менеджерів кодів доступу на зразок 1Password. Хоча додатки в App Store проходять процедуру верифікації, в даному випадку модератори Apple не помітили попадання шкідливого коду в їх систему. На думку дослідників в Palo Alto Networks, в порівнянні з іншими вірусами, створеними для iOS, поведінка XcodeGhost було не таким вже й підозрілим. Метою впровадження вірусних програм до файлової системи iOS є отримання доступу до особистої інформації, паролів доступу до банківських сервісів і платіжних систем, стеження за користувачем, розсилка спаму і реклами тощо. Вберегтися від втручання зловмисників у роботу мобільних пристроїв Apple можна, ретельно дотримуючись правил безпеки:

- не використовувати модифіковані версії iOS;
- своєчасно оновлювати операційну систему після появи офіційних версій;
- для встановлення нових додатків користуватися лише AppStore, звертати увагу на відгуки інших користувачів.

7. Використання пристрою з модулем NFC як засіб автентифікації

Основною метою цього дослідження є проектування можливості використання телефону або іншого пристрою з NFC як засобу надійної автентифікації і розробка програмного забезпечення для безпечної автентифікації користувача за допомогою NFC. Для поліпшення безпеки автомобільних систем безпеки були введені безліч варіантів використання багатофакторної автентифікації для віддалених сервісів: SMS, TOTP цифрові ключі, спеціальні маркери доступу, але як показано з досліджень вище навіть стійка на перший погляд клієнт-серверна архітектура керування системою безпеки не надає необхідного ступеня безпеки, може мати в собі скриті загрози, бекдори та баги розробників. Такі системи можуть стати складні або незручні в застосуванні, наприклад при верифікації доступу до автомобілю за допомогою SMS, що буде ускладнювати життя господаря автомобіля. Тому пропонується розглянути систему автентифікації за допомогою NFC з можливістю виконувати автентифікацію в один дотик до зчитувача. За основу пропонується взяти пристрої на платформі iOS від компанії Apple, розробки якої описувалися вище, нас цікавлять смартфони, шо підтримують технологію NFC та «розумні» годинники Apple Watch, в яких присутній NFC-модуль, що дозволяє працювати в трьох режимах: зчитування і запису міток, режим p2p та режимі емуляції безконтактної банківської карти. Ці пристрої можуть працювати в режимі емуляції карти, який надає можливість обмінюватися APDU повідомленнями з іншими учасниками. Пристрої також підтримують інші стандарти, що необхідні для створення системи автентифікації: U2F – стандарт для швидкої, зручної та безпечної двофакторної автентифікації за допомогою окремого пристрою. Даний вид автентифікації передбачає наявність у користувача окремого фактора воло-

діння криптоключа. Протокол U2F використовує принцип посилки сервісом унікального challenge і відповіді клієнта з підписом, що використовують алгоритм ECDSA з еліптичної кривої secp256r1. Для роботи програмного модулю системи автентифікації розглянемо систему з використанням NFC в якості додаткової системи до вже встановленої системи сигналізації. Під час реєстрації пов'язаний пристрій власника транспортного засобу посилає іншим учасникам мережі повідомлення про наміри проведення автентифікації до транспортного засобу. Пристрої усіх учасників мережі отримують повідомлення про наміри іншого користувача автентифікуватися. Отримавши повідомлення, користувачі порівнюють передані дані з своїми блоками та визначають, чи валідний запит чи ні, після чого підтверджують транзакцію або ні, як і у випадку з іншою системою, що побудована на основі мережі блокчейн – біткоін. У випадку, коли транзакція буде підтверджена більшістю (більше за 51 % проголосувавших за визнання транзакції валідною). Результат операції повертається тому, хто запитував право на доступ до автомобіля. В якості ініціалізуючої системи виступає смартфон на базі iOs чи годинник Apple watch, що підтримують можливість використовувати технологію NFC для створення каналу зв'язку для проведення автентифікації користувача автомобіля і системи безпеки; у випадку співпадіння даних мітки користувачу буде дозволено поступ. Для користувача така система ще простіша – можна не мати при собі ключа від машини, а смартфон чи годинник багато користувачів мають з собою завжди. Таким чином, за допомогою описаних вище процедур цей додаток можна використовувати для безпечної автентифікації користувача з системами, що будуть підтримувати програмно-апаратну реалізацію системи з наявністю NFC передавача та мобільних операційних систем.

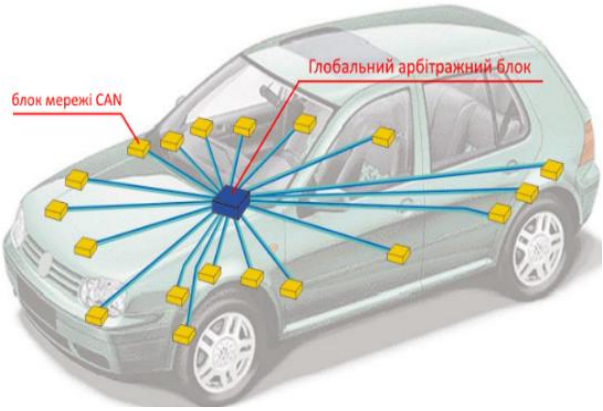

Рис. 2. Централізована схема архітектури попередження вторгнення

Архітектура являє собою мережу, що об'єднує всі блоки між собою, використовуючи спеціальний блок арбітражу, або, як можна його назвати, «глобальний арбітражний блок». Схематично архітектура являє собою систему, що зображена на рис. 2. Основу мережі складає арбітражний блок, який приймає пакети від інших складових блоків мережі CAN, що передають дані один одному. Цей блок визначається найголовнішим блоком в цій системі, якому надані повноваження щодо визначення, чи являються передані дані такими, що саме ці дані були передані від визначеного блоку. Іншими словами, гарантує цілісність даних, що були отримані від блоку, гарантує правильну доставку повідомлення до отримувача та загальну автентифікацію даних, що передаються блоками. Для цього необхідна реалізація системи автентифікації між компонентами системи, яка би являла собою криптографічний протокол встановлення достовірності твердження, що об'єкт у вигляді повідомлення від блоку має очікувані властивості, надавала б гарантії справжності ідентифікаційних даних від блоку, що ініціює передачу. Система повинна виключати можливість реалізації загроз типу «маскарад», «повтор», «підміна» та компрометацію заявленої інформації автентифікації. Розглянемо детальніше захищеність архітектури з глобальним арбітражним блоком від визначених загроз.

Загроза типу «маскарад» полягає в обмані одного об'єкта іншим об'єктом, коли нав'язаний об'єкт видається в якості достовірного, що, наприклад, можливо при перепрограмуванні блоку на необхідні дії, при цьому залишаються параметри, що належать достовірному блоку, тим самим видаючи себе в мережі за достовірний блок. Для захисту від загроз, що належать до такого типу, в системі планується використовувати спеціальні дані у вигляді шифрованого коду автентифікації алгоритмом A5/1.

Загроза типу «повтор» полягає у повторі інформації, що була передана раніше під виглядом нової. Використовувати механізми автентифікації на основі ЕЦП, що було б найкращим рішенням з огляду безпеки, бо ЕЦП забезпечує послугу неспростовності пред'явника найкращим чином, але використання такого виду криптоперетворення не підходить для такого виду системи через його розрахункову складність, бо система має бути побудована на не потужних компонентах. Для захисту від атак типу «повтор» необхідно ввести в систему мітку часу генерації пакету, що дозволяла б ідентифікувати невалідні пакети, якщо ті передаються пізніше ніж закінчився час життя пакета. Додатковою мірою захисту планується введення випадкового значення

Загроза типу «підміна» можлива за умови наявності заздалегідь перехоплених повідомлень від блоку, що необхідно скомпрометувати, або даних арбітражного блоку. Вона зводиться до модифікації істинної обмінної інформації на хибну. Для захисту проти загроз типу «підміна» краще використовувати послугу цілісності, наприклад з використанням для обміну при автентифікації ЕЦП чи коду автентифікації, а також шифрування. В даній архітектурі цю функцію буде використовувати алгоритм шифрування A5/1. Цілісність забезпечується за рахунок використання контрольних сум CRC або функції гешування SHA-1, що дозволяє ефективно захистити цілісність даних та захиститися від атак типу «підміна». Основною перевагою даної архітектури є можливість реалізації системи, що не потребувала б компонентів великої потужності, що робить систему більш економічно та технологічно обгрунтованою для масового використання у виробництві. Оскільки для роботи системи необхідний лише один арбітражний блок високої потужності, що може обробляти усі запити та відповіді від блоків, які передаються від одного до іншого, та виконує роботу з визначення параметрів безпеки передачі повідомлень лише відповідно до даних, що передаються, це дозволяє зменшити навантаження на інші блоки (складові) і дозволяє не робити різні рівні абстракції для мережі CAN, як це реалізовано зараз, але надавати рівень безпеки вищий ніж з використанням рівнів абстракції.

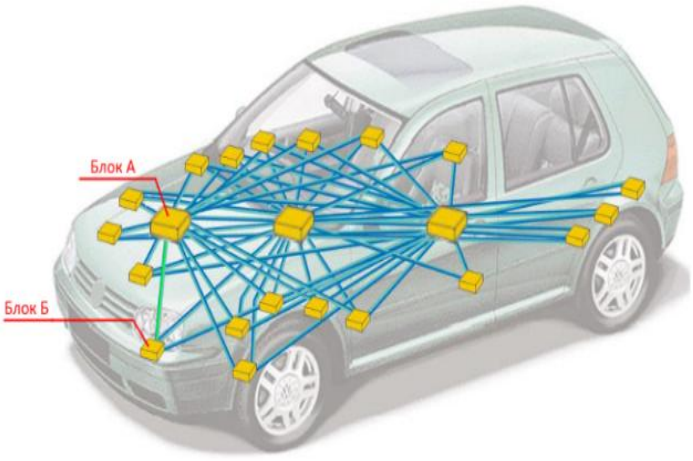

Рис. 3. Централізована схема архітектури попередження вторгнення

У іншому варіанті система представляє собою схожу архітектуру до першої, але її відмінність в тому, що вона побудована на принципах децентралізації та не має будь-яких арбітражних блоків чи рівнів абстракції за будь-якими параметрами зовсім. Схема архітектури зображена на рис. 3. Кожен із блоків являє собою частину децентралізованої мережі, кожен із яких сам відповідає за оброблення параметрів безпеки та визначення захисту від атак. На

рис. 3 показано як блоки А та Б з'єднуються між собою напряму, без будь-яких засобів арбітражу. Кожен з блоків підтримує систему взаємної автентифікації з двома проходами та використовує ідентичні системи гарантування безпеки, використовує базу використаних випадкових чисел, що зберігається на кожному з блоків та гарантує ефективний захист від атаки типу «повтор».

Таким чином, при використанні будь-якої архітектури з описаних можна ефективно забезпечити безпечну та цілісну передачу пакетів у мережі CAN між блоками з можливістю забезпечити ефективну роботу автомобільних систем.

Висновки

Використання технології блокчейн в системі автентифікації автомобіля дозволить розширити можливості безпеки автентифікації для доступу до автомобіля, роблячи цей процес простішим для користувача, бо всі дії можна виконувати за допомогою смартфону, що працює на широко відомій платформі, але ж і підвищується рівень безпеки та довіри, що не вимагає додаткових грошових вкладень, легкий до налаштування та використання та добре захищений від постквантових атак і від інших видів атак, що зараз є дуже загрозливими для безпеки сучасної автоіндустрії. Великим плюсом є, що Apple буде співпрацювати з виробниками автомобілів для CarKey, та є вірогідність виконання версії заводського варіанту, що зробить цю технологію ще більш доступною, простою для потенційних користувачів. Системи безпеки автомобіля будуть мати високий рівень безпеки автентифікації, для реалізації якої використовується децентралізована мережі блокчейн з вузлами для кожного автомобіля, що автентифікують користувача групово та 51 % інших вузлів має підтвердити запит на автентифікацію. В іншому випадку автентифікація буде неможливою і доступу до транспортного засобу надано не буде. Таким чином, вирішуються проблеми автентифікації та безпечності передачі даних між блоками між собою, що перетворює розроблену систему в покращений та надійний захід автентифікації на основі децентралізованої мережі блокчейн та двох комплексних оновлених схем системи передачі критичних даних всередині автомобіля.

Список літератури:

1 NISTIR 8202. Blockchain Technology Overview / NIST // NISTIR. Gaithersburg : US Department of Commerce, 2017. P.1-26.

2. Brown. Vehicle Security Systems // Build Your Own Alarm and Protection Systems. Newnes, 1601996. P. 7 – 155.

3. Knight A., Hacking Connected Cars: Tactics, Techniques, and Procedures. K. : Information Systems, 2019. P. 5-250

4. Car Security 101 [Електронний ресурс]. Режим доступу: www/ URL: https://www.lifewire.com/car-security-101-534872 – 01.05.2020 р.

Надійшла до редколегії 03.10.2020

Відомості про авторів:

Горбенко Іван Дмитрович – д-р техн. наук, професор, професор кафедри безпеки інформаційних систем і технологій, факультет комп'ютерних наук, Харківський національний університет імені В.Н. Каразіна, головний конструктор АТ «Інститут інформаційних технологій», Україна; e-mail: GorbenkoI@iit.kharkov.ua, ORCID: https://orcid.org/0000-0003-4616-3449

Фесенко Дмитро Олександрович – магістрант, кафедра безпеки інформаційних технологій, факультет комп'ютерної інженерії та управління, Харківський національний університет радіоелектроніки, Україна; e-mail: ddfff21@gmail.com