DOI: 10.58254/viti.6.2024.21.250

УДК 004.056.5

д-р техн. наук, ст. наук. співр. Чевардін В. Є. ORCID:0000-0002-1070-4568 (ВІТІ ім. Героїв Крут)

ОРГАНІЗАЦІЙНО-ТЕХНІЧНІ РІШЕННЯ ЩОДО ПОБУДОВИ ЗАХИЩЕНИХ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ

В роботі розглянуті основні підходи до побудови архітектури відкритих ключів PKI з розділенням на базову, дворівневу та багаторівневу ієрархії. Розглянуті сучасні способи атак на існуючі інфраструктури відкритих ключів, протоколи побудови захищених з'єднань як провідних так і безпровідних систем.

Визначені основні класи атак на інфраструктури PKI, з яких основна увага приділена найбільш небезпечному класу атак – людина посередині (MITM-атакам). В роботі наведено моделі різних класів MITM-атак, їх деталі та існуючі способи зменшення ризиків їх реалізації.

Також наведені існуючі приклади успішних атак на компанії та різні організації, які реалізовували моделі MITM-атак на прикладному, мережевому та фізичному рівні моделі міжмережної взаємодії. Для інфраструктури PKI одним з варіантів наводиться її сегментування, що дозволяє зменшувати масштаби впливу атаки на центр сертифікації ключів.

Також у роботі наведено альтернативний спосіб захисту від MITM-атак з використанням технології розподіленого мікрореєстра (DLT) для створення децентралізованих систем розповсюдження криптографічних ключів (DKMS). Рішення базується на використанні мікрореєстрів (distributed micro ledger technology – DMLT). Застосування DMLT для створення DKMS дозволяє забезпечити захист від більшості класів MITM-атак.

Ключові слова: *інфраструктура відкритих ключів, протоколи захисту інформації, уразливості протоколів, атаки MITM.*

V. Chevardin Organizational and technical solutions for the construction of protected information and communication systems.

The paper presents the main approaches to the construction of the PKI public key architecture divided into basic, two-level, and multi-level hierarchies. Modern methods of attacks on existing public key infrastructures, protocols for building secure connections of both wired and wireless systems are considered.

The basics of the class of attacks on PKI infrastructures are defined, of which the main attention is paid to the most dangerous class of attacks – man-in-the-middle (MITM-attacks). The paper provides models of various classes of MITM attacks, their details and existing methods of reducing the risks of their implementation. Existing examples of successful attacks on enterprises and various organizations that implemented MITM attack models at the application, network, and physical levels of the network interaction model are also given.

For the PKI infrastructure, one of the options is its segmentation, which allows to reduce the scope of attacks on the key certification center. The paper also provides an alternative way to protect against MITM attacks using distributed micro ledger technology (DLT) to create a decentralized cryptographic key distribution system (DKMS). The solution is based on the use of micro ledgers (distributed ledger technology – DMLT). Using DMLT to create a DKMS allows protection against additional classes of MITM attacks.

Keywords: *public key infrastructure, information protection protocols, protocol vulnerabilities, MITM attacks.*

Актуальність досліджень. Аналіз існуючого стану застосування систем кібербезпеки та захисту інформації, що використовуються в інформаційних системах спеціального призначення, показав гостру потребу в підвищенні ефективності процесів аналізу уразливостей існуючих систем захисту інформації та прийняття відповідних рішень щодо їх усунення урядовими та регіональними командами реагування на кіберзагрози. Брак фінансування, матеріального та інформаційного забезпечення військ, сил, викликало потребу в розробці нових наукових засад та підходів щодо підвищення кіберготовності та кіберзахищеності інформаційно-комунікаційних систем держави. В зв'язку з цим, створення стійких до кібервпливів інфраструктурних рішень щодо побудови інформаційно-комунікаційних систем є єдиним способом забезпечення кібербезпеки та структурної надійності інформаційно-комунікаційних систем об'єктів критичної інфраструктури держави. Це можливо зробити шляхом побудови інформаційного середовища для отримання розвідувальної інформації, передачі інформації для управління системами озброєння та військової техніки, а також для проведення інформаційно-психологічних та кібероперацій.

Основою таких систем є єдина платформа формування захищених комунікаційних зв’язків з надійною інфраструктурою відкритих криптографічних ключів, генерації ключових послідовностей, шифрування та розшифрування даних, забезпечення функцій автентифікації суб’єктів та об’єктів доступу, моніторингу процесів у системі з обов'язковим резервуванням критичних елементів та даних.

Результати аналізу хибних підключень громадян України до мережі Інтернет та порушення доступності ресурсів Інтернет дозволили визначити найбільш розповсюджену загрозу, відому як атака "men in the middle". MITM-атака реалізується різними способами, а саме створенням хибних базових станцій мобільного зв’язку, хибних центрів розподілу криптографічних ключів, хибних dns-серверів, arp-серверів та іншими способами [1–4]. Для існуючих підходів з централізованим розподілом криптографічних ключів, таких як інфраструктура відкритих ключів PKI, цей клас атак створює загрозу перехоплення відкритих ключів та їх підміни або блокування між головним сервером та будь-яким клієнтом, що робить уразливим практично всі організаційно-технічні структури, що використовують PKI. В зв’язку з чим, виникла потреба в пошуку альтернативних підходів до побудови схем генерації та розповсюдження криптографічних ключів з підвищеною захищеністю до MITM-атак.

Метою даної роботи є розробка нового підходу до побудови інфраструктури відкритих криптографічних ключів зі зменшенням ризику втрати конфіденційності, цілісності та доступності ресурсів інформаційно-комунікаційної системи в умовах диверсифікації MITM-атак.

1. Викладення матеріалу

Розглянемо основні елементи інфраструктури PKI, які забезпечують функції електронного цифрового підпису та автентифікації для інформаційно-комунікаційних мереж та систем.

Цифрові сертифікати – це цифрові файли, які забезпечують можливість ідентифікації (організації, особи, служби або програмного коду) та автентичності відкритих ключів шифрування та цифрового підпису. Цифрові сертифікати поділяються на типи:

сертифікати SSL/TLS для перевірки домену (DV), перевірки організації (OV), розширеної перевірки (EV);

сертифікати підпису коду;

сертифікати підпису документів;

сертифікати підпису електронної пошти (S/MIME);

сертифікати автентифікації клієнтів.

Ключові пари – це криптографічні елементи шифрування/розшифрування даних, підпису/верифікації даних, які складаються з публічного (відкритого) та особистого (секретного) ключів.

Органи сертифікації – це, як правило, центр сертифікації (ЦС), яких може бути для однієї організації один або декілька. Залежно від розміру організації та ієрархічної структури ЦС можуть поділятися на: кореневий ЦС, проміжний ЦС та ЦС видачі (може також бути одночасно і проміжним).

За архітектурною особливістю PKI може поділятися на загальнодоступну PKI (Public CA) та приватну (Private CA).

Загальнодоступна PKI використовується для забезпечення захисту браузерів, месенджерів, програмного коду, електронної пошти та інших інформаційних систем загального призначення, як правило, з використанням протоколу SSL/TLS.

Приватна PKI використовується для забезпечення захисту для внутрішніх мереж, доступу користувачів до ресурсів інформаційних систем, використання приватних та внутрішніх Wi-Fi мереж організації, мобільних пристроїв користувачів. Для цього, як правило, використовують приватні PKI, кореневі сертифікати яких встановлюються на кожному

пристрої. Однією з загроз для такого варіанта розгортання PKI є компрометація секретних ключів кореневого сертифікату, що створює загрозу всій інфраструктурі організації і потребує відкликання всіх сертифікатів, підписаних з використанням цифрового підпису кореневого центру сертифікації. Для зниження ризиків втрати конфіденційності інформації, що циркулює в організації, здійснюють розділення PKI інфраструктури на сегменти. Розглянемо варіанти.

Базова однорівнева архітектура PKI наведена на рисунку 1, яка побудована на використанні Кореневого Центру Сертифікації (КЦС), який забезпечує функції захисту для всіх користувачів організації.

Рис. 1. Базова однорівнева архітектура PKI

Базова дворівнева архітектура PKI наведена на рисунку 2.

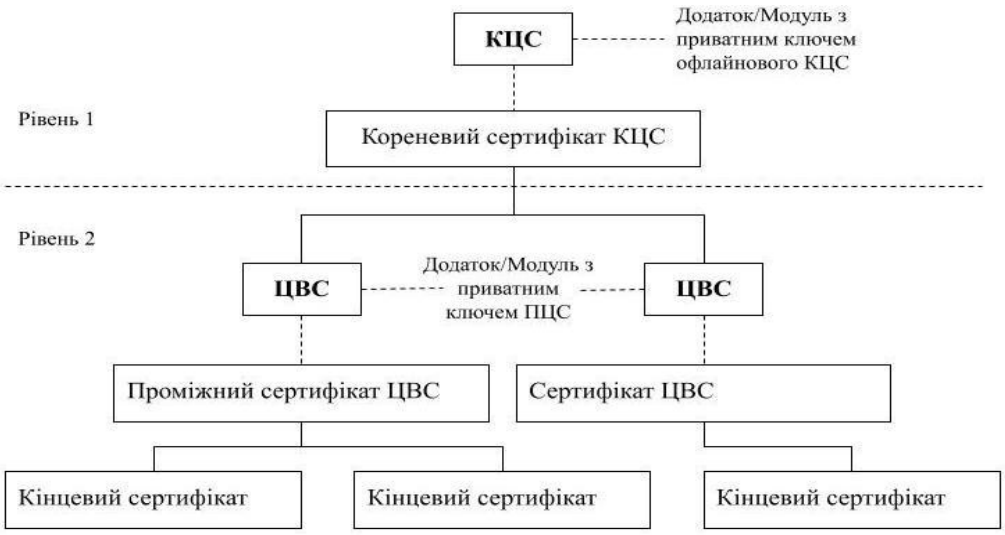

Рис. 2. Базова дворівнева архітектура PKI

Базова дворівнева архітектура PKI побудована на використанні офлайнового (недоступного всім користувачам через мережу Інтернет) Кореневого Центру Сертифікації (КЦС), який підписує сертифікати відкритих ключів центрів видачі сертифікатів (ЦВС). Генерацію цифрового підпису на рівні 2 здійснюють ЦВС, які забезпечують функції захисту для всіх користувачів організації. Між собою ЦВС зв'язуються через мережу Інтернет.

Базова трирівнева архітектура PKI побудована на використанні офлайнового КЦС, який підписує сертифікати проміжних центрів сертифікації (ПЦС) на рівні 2 (без використання мережі Інтернет). Генерацію цифрового підпису та підпис сертифікатів для всіх ЦВС на рівні 3 здійснюють ПЦС. Між собою ПЦС зв'язуються через мережу Інтернет. Для всіх ЦВС (3-й рівень) сертифікати підписують з секретними ключами ПЦС. ЦВС видають сертифікати кінцевим користувачам. Використання трирівневої архітектури дозволяє зробити окремі

сегменти сертифікації користувачів в організації. Це знижує ризик блокування або компрометації конфіденційної інформації користувачів у випадку компрометації секретного ключа одного з ПЦС або ЦВС. У разі компрометації секретного ключа ЦВС під загрозу компрометації ключів користувачів підпадає лише один сегмент мережі організації (рис. 3), що є перевагою над базовою однорівневою архітектурою, з одного боку. З іншого боку, трирівнева або багаторівнева архітектура вимагає збільшення витрат на підтримку та забезпечення роботи ПЦС, ЦВС та захист каналів обміну сертифікатами між ними.

Базова трирівнева архітектура PKI наведена на рисунку 3.

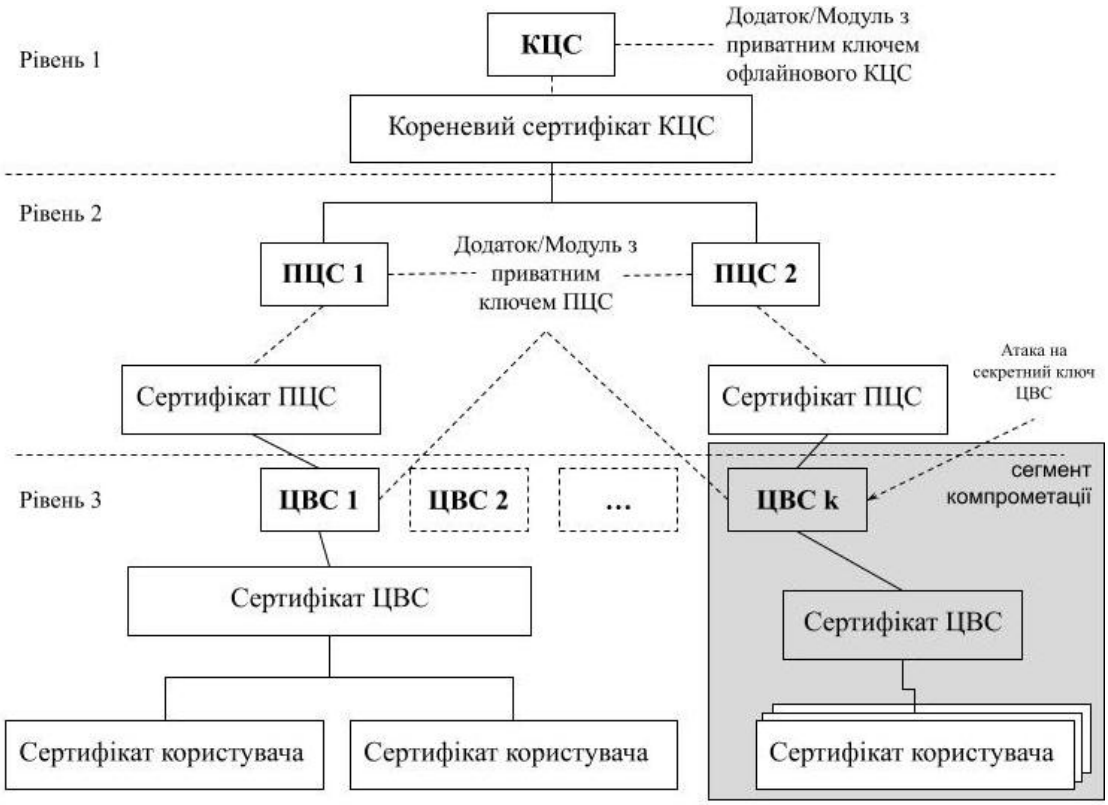

Рис. 3. Базова трирівнева архітектура PKI

Основним етапом атак на інфраструктури PKI сьогодні є захоплення контролю кореневих сертифікатів організацій та окремих користувачів, що надає зловмиснику можливість відкликання, блокування, створення нових сертифікатів користувачів. Розглянемо більш детально етапи сучасних атак на елементи та протоколи захисту інформації та інфраструктури PKI.

Класи атак на PKI

Клас атак на відмову в обслуговуванні (Dos атаки) (порушення доступності):

атаки на центр сертифікації (CA DoS) спрямовані на перевантаження ЦС запитами або запуск DDoS атак, що порушує видачу та перевірку сертифікатів;

атаки на відповідача протоколу статусу онлайн-сертифіката (OCSP DoS), спрямовані на перевантаження ЦС запитами протоколу OCSP, що блокує можливість перевірки користувачами дійсність сертифікатів.

Клас атак на основі фішингу та соціальної інженерії.

Атаки на основі використання методів та технік соціальної інженерії та фішингових розсилань пошти з шкідливим вкладенням, прикладом такої атаки є атака на домен live.com, яка була здійснена шляхом надсилання електронного листа на легальну адресу, включену до

дозволених адрес відповідно вимог CA/Browser Forum Baseline Requirements. Зловмисник зміг зареєструвати ту ж саму адресу, що дозволило йому схвалити використання домену.

Клас атак на секретний ключ користувача (порушення конфіденційності):

атаки на основі викрадення секретних ключів (Private Key Theft). Цей клас атак оснований на різних техніках, спрямованих на викрадення секретних ключів власників сертифікатів, що надає змогу зловмиснику видавати себе за легального користувача захищеної системи та здійснювати подальші шкідливі дії від його імені;

атаки на основі використання зловмисного програмного засобу (Keylogging) для захоплення інформаційних потоків від засобів введення інформації на ПЕОМ користувачів. Ці атаки дають можливість реалізувати сценарій MITM-атаки зі створенням хибного ключа легального користувача або викраденням ключа легального користувача.

Клас атак з використання компрометації центру сертифікації (порушення конфіденційності), які реалізують модель MITM-атаки:

атаки на основі створення фальшивих сертифікатів центру сертифікації, який був зламаний або мав критичну уразливість, яка дає можливість його експлуатації. Прикладом реалізації цієї атаки є використання утиліти Certipy, розробленої Олівером Ляком, для експлуатації уразливості сертифікатів Active Directory (AD CS), яка знаходить уразливі шаблони сертифікатів та надає зібрані дані у форматі BloodHound та json, а саме: CA Name, DNS Name, Certificate Subject, Certificate Validity Start & End, Access Rights & Permissions, Vulnerable Certificate Name, Vulnerabilities. У разі успішної атаки отримують геш NTLM адміністраторів, який можна використовувати для автентифікації та компрометації контролера домену;

атаки на основі створення фальшивого ЦВС для видачі підроблених сертифікатів. Прикладом цієї атаки вважається випадок з компанією Lenovo. До переліку довірених центрів сертифікації Lenovo було включено центр сертифікації Superfish CA. Виявлена уразливість програмно-апаратних засобів мала місце у користувачів, які користуються застарілими програмно-апаратними засобами та браузерами Firefox. Для захисту від такої уразливості в програмі Windows Defender є оновлення, яке видаляє додаток Superfish. Слід зазначити, що сертифікат для Superfish CA, підписаний компанією Komodia, не виключає наявність уразливостей в інших додатках з сертифікатами, підписаними компанією Komodia, таких як My Family Secure, Kurupira Webfilter.

Клас атак з відкликанням сертифікатів (порушення цілісності), які реалізують модель MITM-атаки:

атаки на основі маніпуляцій зі списками відкликаних сертифікатів (CRL) здійснюються з метою запобігання виявлення користувачами відкликаних сертифікатів. Це призводить до використання клієнтами скомпрометованих або тих, що втратили чинність сертифікатів відкритих ключів. В разі чого зловмисник може скористатися уразливими або скомпрометованими ключами клієнтів та отримати доступ до інформації або послуг цифрового підпису клієнта жертви;

атаки на основі маніпуляції відповідача протоколу статусу онлайн-сертифіката (OCSP) з метою надання хибної інформації щодо статусу сертифіката. В разі чого зловмисник може маніпулювати статусом сертифікатів та примушувати клієнтів використовувати свої сертифікати, внаслідок чого також отримати доступ до інформації або послуг цифрового підпису клієнта жертви.

Nicolas Serrano, Hilda Hadan, L. Jean Camp [7] провели аналіз інцидентів, пов'язаних з роботою центрів сертифікації відкритих ключів з великою кількістю сертифікатів, а саме Let's Encrypt – 92,300,644, Sectigo – 27,859,495 DigiCert – 12,577,372, GoDaddy – 2,476,593, GlobalSign – 680,249 Amazon – 644,901 та інших. Найбільша кількість інцидентів, пов'язаних з ЦВС, прийшлася на DigiCert, Comodo, Symantec, WoSign, Camerfirma. Однією з основних

причин інцидентів стали невідповідність полів сертифікатів вимогам базового рівня безпеки, що склали 38.52 %, невідповідність базовому рівню безпеки відповідачів проколу статусу сертифікатів OCSP та списку відкликаних сертифікатів (CRL), які склали 10.29 %, атаки на основі видачі фальшивих сертифікатів склали 4.75 %, атаки на основі зниження рівня безпеки, а саме використання 512/1024 біт ключа протоколу RSA (4.75 %), використання алгоритму SHA-1/MD5 (3.96 %).

Клас атак на основі вразливостей криптографічних протоколів, які реалізують модель MITM-атаки:

атаки на основі використання слабких криптографічних ключів. Цей клас атак використовує нестійкі параметри криптографічних систем. Прикладом експлуатації уразливостей протоколів асиметричної криптографії є факторизація експортованих RSA-ключів (FREAK), шляхом деградації стійких RSA-ключів до нестійких (export grade RSA) з послідовним зламом. Прикладом експлуатації вразливостей геш-функцій є пошук колізій та атак на алгоритм SHA-1. Прикладом експлуатації уразливостей алгоритмів потокового шифрування є атаки на симетричні криптоалгоритми RC4 та схеми генерації спільного секрету DHE. Сьогодні можна знайти багато сайтів, які працюють на сертифікатах, отриманих до 2015 року, або дозволяють використовувати сертифікати, що створені з використанням SHA-1, або 512 бітових RSA-ключів;

атаки на основі використання застарілих протоколів криптографічного захисту інформації. Прикладом такої атаки став випадок коли зловмисник зміг узгодити в протоколі використання застарілої версії TLS протоколу (уразливість CVE-2014-3511). Цей тип атак розповсюджений за причиною частого використання організаціями застарілого обладнання.

Клас атак з використанням нового ключа користувача, які реалізують модель MITM-атаки. Одним з прикладів таких атак є порушення цілісності протоколу handshake, під час якої зловмисник імітує нового користувача інформаційної системи та намагається діяти від його імені для отримання конфіденційної інформації від справжніх користувачів мережі. Як правило, виділяють три типи атак цього класу:

атаки на основі викрадення сесій. Цей клас атак дають можливість зловмисникам перехоплювати та маніпулювати зв'язками між двома користувачами, надаючи фальшивий сертифікат з метою подальшого прослуховування або зміни даних;

атаки на основі підробки сертифікатів. Цей клас атак оснований на використанні нових шахрайських сертифікатів з метою представлення зловмисника легальним сервером чи службою, що надають послуги ЕЦП, використання яких жертвою призводить до втрати конфіденційності інформації, що передається захищеними каналами. Прикладом такої атаки став випадок Gogo Found Spoofing Google SSL Certificates, який був виявлений у компанії Gogo, яка надавала послуги служби захисту Інтернет з'єднань Gogo Inflight Internet. Ця служба використовувала сертифікати SSL MITM для контролю під'єднання користувачів для відвідування сайтів Google та ресурсів YouTube. В результаті цих дій компанія Gogo мала потенційні можливості для отримання даних клієнтів Інтернет послугами. Використання попереджень від служби безпеки браузерів, які викликають підозру відповідно до політики безпеки Gogo Inflight Internet, можуть блокувати та знищувати законні SSL сертифікати та послаблювати моделі довіри браузерів користувачів.

Таким чином, кожен з розглянутих типів атак на інфраструктуру PKI може представляти більшу чи меншу загрозу для організації, що залежить від типу архітектури PKI, реалізованої в організації. Але найбільшу загрозу складають класи MITM-атак та атак на основі ураливостей криптографічних протоколів. Результати проведеного огляду показали найбільшу кількість атак, пов'язану з наступними причинами: закладні програмні засоби (Software bugs) – 24 %, невідповідність вимогам або неправильна інтерпретація (Believed to be compliant, Misinterpretation, Unaware) – 18 %, бізнес процеси, уразливості конфігурації центрів

видачі сертифікатів та тестування (Business model, CA decision, Testing) – 13 %, людські помилки (Human error) – 9 %, решта причин склали менше 8 %.

В зв'язку з цим, для визначення шляхів підвищення захищеності та надійності PKI, треба дослідити варіанти реалізації MITM-атак та існуючі уразливості криптографічних протоколів.

Способи реалізації атак класу MITM

Спосіб реалізації MITM-атаки 1

Розглянемо варіант 1 проведення MITM-атаки на користувачів Інтернет, які працюють за стандартними протоколами міжмережної взаємодії. Під час встановлення з'єднання між користувачами та сервером зловмисник виступає посередником для обох сторін. Як правило, метою зловмисника є підміна кореневого сертифікату відкритого ключа серверу на хибний відкритий ключ з метою подальшого прослуховування трафіку або нав'язування хибної інформації. Варіант цієї атаки наведено на рис. 4. шляхом порівняння етапів роботи протоколу Handshake та варіанта етапів роботи протоколу Handshake з втручанням зловмисника на етапі створення сесійних ключів користувача.

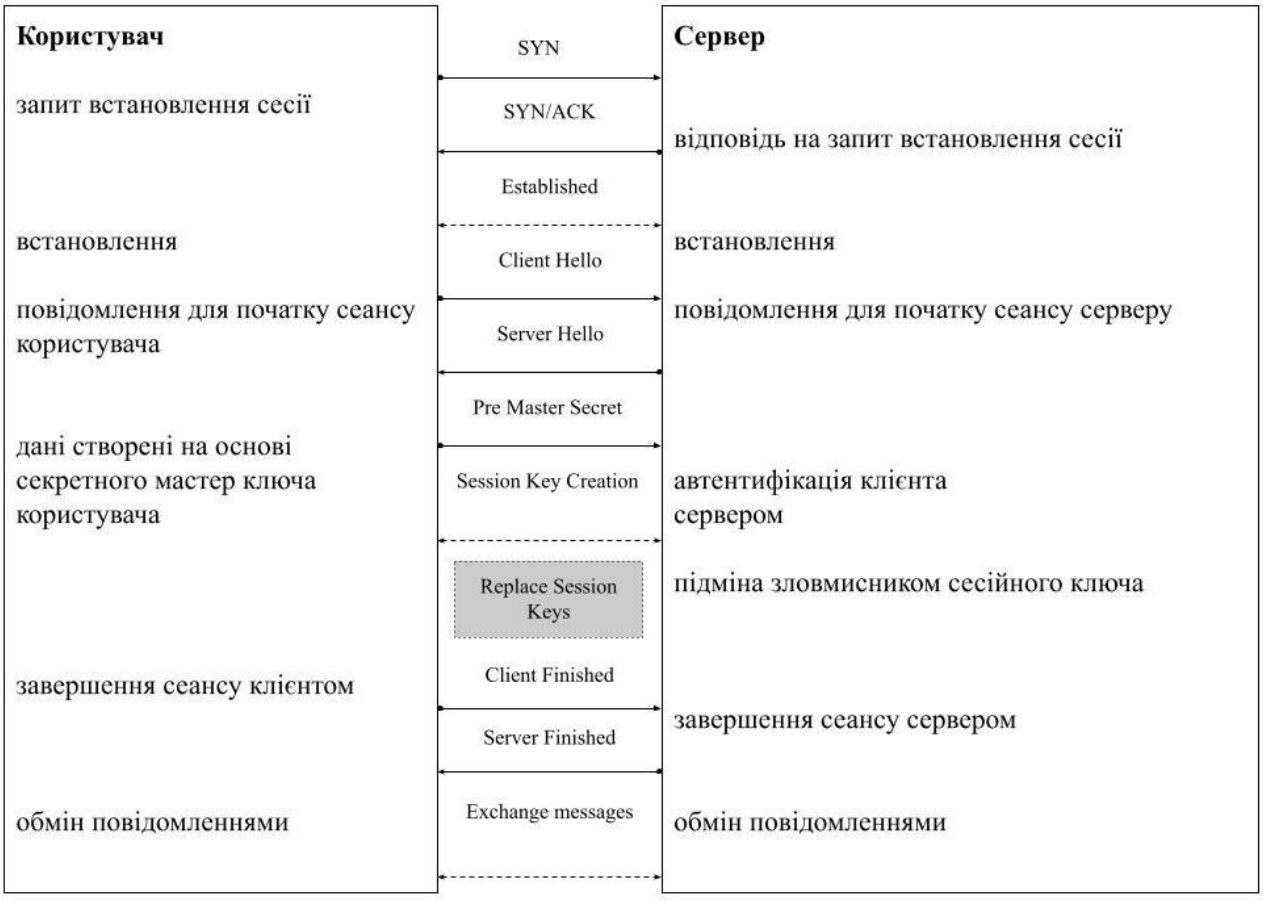

Рис. 4. Модель MITM-атаки на протокол SSL Handshake
порівняно з кроками класичного протоколу SSL Handshake

З рисунка 4 можна побачити місце, з якого зловмисник впливає на процедуру Handshake. На етапі створення сесійного ключа, під час автентифікації клієнта сервером, зловмисник надає свою інформацію для отримання сесійного ключа від серверу. Для справжнього клієнта зловмисник надає інший ключ згенерований власноруч. Після підміни сесійних ключів зловмисник становиться ретранслятором всього трафіку від серверу і до серверу для клієнта жертви.

Спосіб реалізації MITM-атаки 2

Атака на основі вразливості протоколів WPA2 або WPA3 (Wifi-Eavesdropping), яка реалізується прослуховуванням сесій (встановлення з’єднань) в Wi-Fi мережі. Для реалізації цього варіанта MITM-атаки використовують користувачів, що підключаються, як правило, до публічних мереж та мають обладнання бездротового доступу з дозволом переспрямування ICMP трафіку (рис. 5). За таким сценарієм зловмисник може визначати IP-адресу, відкриті UDP-порти користувача (жертви) та серверу, з яким він намагається зв’язатися. Зловмисник може надсилати підроблені пакети, використовуючи вихідну IP-адресу точки доступу.

Прикладом такої атаки є використання вразливості CVE-2022-25667, яка використовує іншу вразливість, пов’язану з уразливостями схем та протоколів автентифікації CWE-287. Приклад класу уразливостей CWE-287: CVE-2021-35033 – уразливість програмного забезпечення маршрутизатора Wi-Fi, яке використовує жорстко закодований пароль для оболонки BusyBox, що дозволяє обходити автентифікацію через порт UART; CVE-2021-35395 – уразливість програмного забезпечення в модулях SFK, реалізоване за рахунок переповнення буфера на основі стека мікросхеми Wi-Fi модуля, що використовується для IoT пристроїв та інші.

Рис. 5. Атака на основі прослуховування бездротової Wi-Fi мережі (Wifi-Eavesdropping)

За узагальненими даними від www.cve.details, www.mitre.org, www.cve.org уразливість CVE-2022-25667, знайдена в 89 % найбільш розповсюджених Wi-Fi маршрутизаторах. Ця уразливість дозволяла здійснити MITM-атаку на протоколи бездротового доступу з використанням Wi-Fi модулів.

Спосіб реалізації MITM-атаки 3

Атака на основі вразливості протоколів WPA2 або WPA3, яка реалізується шляхом викрадення сесії (встановлення з'єднань) в Wi-Fi мережі (Session Hijacking). Для реалізації цього варіанта MITM-атаки зловмисник перехоплює сесію легального користувача, використовуючи два сценарії викрадення сесій: захоплення сесії (Session Side Jacking) та Cross-Site Scripting (XSS).

Спосіб реалізації MITM-атаки 4

Атака на основі вразливості протоколу HTTPS (HTTPS Spoofing), яка також називається омографічна атака. Цей тип атаки будується на підміні справжньої адреси сайту на хибну, шляхом використання певних символів коду, наприклад, ASCII. Як правило, звичайний користувач не відрізняє хибну адресу від справжньої.

Спосіб реалізації MITM-атаки 5

Цей клас атак основний на уразливості програмного забезпечення OpenSSL, яке є базовою програмною платформою побудови протоколів захисту інформації для багатьох протоколів та сервісів: OpenVpn, SSL, TLS та операційних систем: Windows, Linux, IoS. Прикладом, цього варіанта MITM атаки є експлуатація уразливості CVE-2015-1793, а саме знаходження для бібліотеки програмних функцій OpenSSL версій 1.0.2b, 1.0.2c, 1.0.1n і 1.0.1o можливості використання альтернативного ланцюжка сертифікатів, який містить сертифікати зі слабкими ключами, які мають прапорець CA flag з позначкою "issue", що призводить до появи уразливості в усіх програмах, що використовують сертифікати SSL, TLS і DTLS. В такому випадку зловмисник стає довіреною стороною, як звичайний центр сертифікації ЦВС, що видав недійсні загальнодоступні сертифікати SSL/TLS для будь-якого домену в мережі Інтернет.

Спосіб реалізації MITM-атаки 6

Цей клас атак основний на примусовому пониженні версії протоколу MITM TLS та маніпулювання ARP-таблицями. Це досягається в декілька кроків:

крок 1 – визначення MAC адреси машини жертви, де Користувач А запитує кожен пристрій у мережі, запитуючи: «Хто використовує цю адресу IP_B?» Користувач В генерує відповідь користувачу А, "IP_B використовує MAC-адресу MAC_B". Користувач А отримує відповідь і оновлює свій ARP-кеш для створення пари IP_B та MAC_B. Користувач А тепер використовує MAC_B для надсилання даних користувачу В.

Враховуючи, що кешовані ARP-таблиці оновлюються за відповіддю навіть без запиту, без автентифікації повідомлень або перевірки цілісності, це дає можливість зловмиснику підробити інформацію в даній відповіді для перехоплення сеансу та маніпулювання ARP-таблицями.

Крок 2 – маніпулювання таблицями кешу ARP-пристрою, де Користувач С (зловмисник) надсилає відповідь користувачу А, наступного змісту: "IP_B використовується MAC-адресою MAC_C". Щоразу, коли Користувач А бажає зв'язатися з користувачем В, він надсилає дані через користувача С. Користувач С надсилає відповідь користувачу В, з наступним змістом: "IP_A використовується MAC-адресою MAC_C". Щоразу, коли користувач В бажає зв'язатися з користувачем А, він надсилатиме дані через користувача С.

Тепер користувач С отримує всі пакети, надіслані між користувачами А і В (наприклад, між АРМ клієнта і маршрутизатором). Користувач С може увімкнути переадресацію IP для перенаправлення всього отриманого трафіку на відповідний пристрій для перехоплення, зміни або скидання отриманих пакетів. Це використовується для зловживання функцією браузерів для узгодження попередніх версії SSL/TLS. Атака MITM завершена.

Спосіб реалізації MITM-атаки 7

Цей тип MITM-атак заснований на зниженні версії протоколу TLS під час встановлення з'єднання за протоколом рукостискання, який вже розглядався раніше. Для цієї атаки

використовується сценарій з примусовим зниженням версії протоколу TLS, що призводить до появи уразливості в самому протоколі старої версії.

Протокол рукостискання, це відомий, що починається з “ClientHello”, де користувач А (клієнт) надсилає користувачу В (серверу) версію SSL або TLS. У застарілих версіях SSL (версія 2) цей пакет рукостискання можна було перехопити та змінити, але для версії SSLv3 це вже неможливо сьогодні. Сучасні браузери підтримують SSLv3 до TLSv1.2, але використовуватимуть найвищу версію, яку підтримує сервер. Користувач С (зловмисник) не може безпосередньо змінювати будь-які пакети, надіслані під час рукостискання, але може перехоплювати та скидати певні пакети, змусивши браузер вважати, що користувачу В (сервер) не підтримує певну версію SSL/TLS, внаслідок чого знизити узгоджену версію.

Приклад.

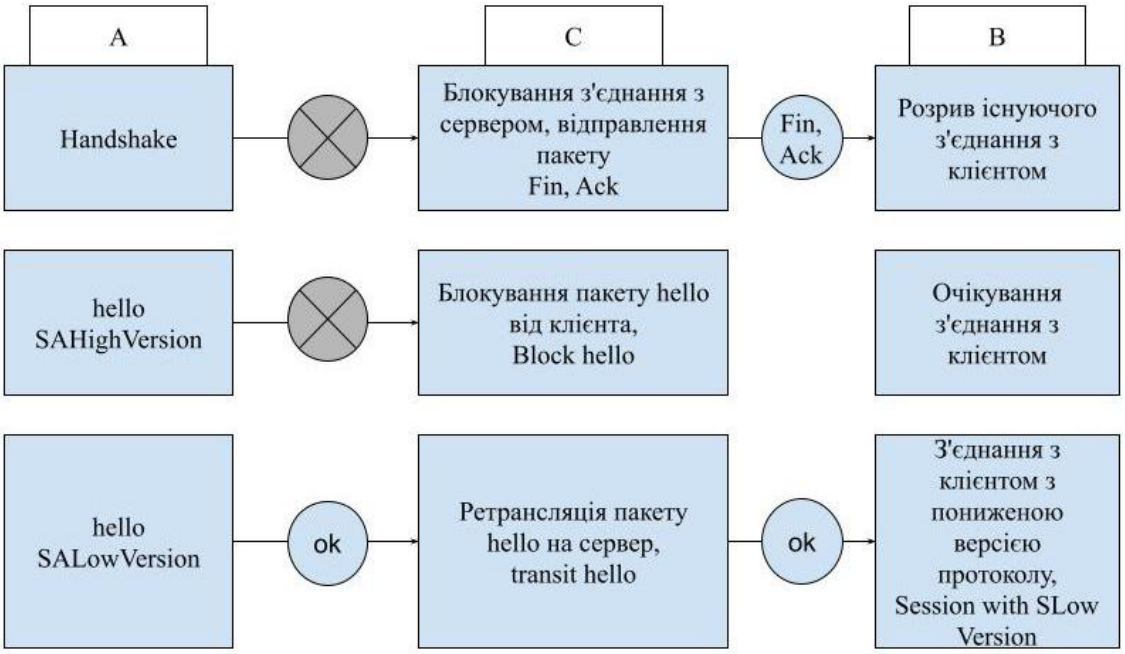

Рис. 6. Схема MITM-атаки заснована на зниженні версії протоколу TLS під час встановлення з’єднання за протоколом рукостискання

Користувач А надсилає «ClientHello» на сервер.

Користувач С перехоплює та скидає пакет (у разі встановлення нової сесії).

Користувач С відкидає поточний пакет рукостискання.

Користувач С надсилає TCP-пакет «FIN, ACK» користувачу В, що припиняє діюче підключення.

В результаті Користувач А повторно намагається підключитися, надсилаючи ”ClientHello” з однією з попередніх версій SSL/TLS. Атака MITM завершена.

Атаки з пониженням версії протоколу базуються на припущенні, що помилка або припинення з’єднання означає збій з’єднання через збій протоколу SSL/TLS. Крім того, для забезпечення сумісності з попередніми версіями SSL/TLS Користувач А може спробувати створити кілька з’єднань, доки не буде встановлено успішне з’єднання.

Таким чином, Користувач С, повторюючи зниження версії протоколу, може переконати Користувача А узгодити SSLv3 із Користувачем В. Ця атака на пониження версії протоколу була перевірена під час підключення до Facebook за допомогою останніх версій Firefox, Chrome і Opera.

Іншим прикладом MITM-атаки є експлуатація уразливості Oracle з операційною системою Ubuntu 14.04 (CVE-2016-2107), для усунення якої було запропоновано Fix OpenSSL Padding Oracle vulnerability (CVE-2016-2107) – Ubuntu 14.04. Деталі цієї атаки та рекомендації щодо захисту описані в [8, 9].

Сценарії захисту від MITM-атак

Способами зменшення шкоди від реалізації MITM-атаки є розділення мережі на зони зберігання та використання відповідних пар ключів, що зменшує кількість клієнтів, які можуть стати жертвами атак нав'язування або порушення конфіденційності даних. Це удосконалення описаної системи за рахунок створення альтернативної інфраструктури відкритих ключів зі зменшенням ефекту розповсюдження зони дії атаки за рахунок сегментації інфраструктури. Розглянемо варіант побудови інфраструктури PKI з урахуванням особливостей розглянутих класів MITM-атак.

Сценарій 1

Одним із перших рішень було використання HTTP Public. Закріплення ключа (HTTP Public Key Pinning-HPKP) або закріплення сертифіката. За допомогою цього механізму вебхост буде надсилати один або більше криптографічних ідентифікаторів (відкритий ключ або сертифікат) для агента користувача (веббраузер) у HTTP-заголовку. Наприклад, це може бути відкритим ключем сертифіката домену або відкритим ключем у його ланцюжку довіри). Агент користувача зберігає ідентифікатор на деякий час, перевіряючи його ідентичність, яку пропонує хост кожного разу, коли користувач відвідує його із закріпленим ідентифікатором. Ця схема уможливила виявлення фальшивих сертифікатів. Так, один із найпомітніших випадків був в організації “DigiNotar-2011”.

Одним з захисних механізмів, який замінив закріплення сертифікату, став новий атрибут – прозорість сертифіката (Certificate Transparency). Цей механізм дозволяє перевіряти сертифікати клієнтів на предмет виявлення фальшивих, але не захищає від появи нових шахрайських сертифікатів. Цей недолік можна позбавитися шляхом використання центрів сертифікації для кожного домену, які перевіряють фальшиві сертифікати. В такому випадку веббраузери не є центральним органом контролю, але мають повноваження застосовувати політику журналювання.

Враховуючи, що ЦС не є обов’язковим для реєстрації нещодавно виданих сертифікатів у журналах Certificate Transparency (CT), деякі кореневі програми вимагають цього, щоб довіряти цифровому сертифікату. Наприклад, коренева програма Google, для якої часова позначка підписаного сертифіката SCT (Signed Certificate Timestamps) видається кожного разу, коли центр сертифікації надсилає новий сертифікат до журналу CT, а згодом кожна позначка SCT додається до відповідного сертифіката для перевірки помилкових полів. Недоліком цього підходу є відсутність можливості запобігти іншим загрозам порушення цілісності журналів CT та справжності часових міток SCT, у випадку відсутності системи реєстрації подій.

Сценарій 2

Окремим підходом до підвищення стійкості та надійності інфраструктури відкритих ключів є використання спеціальних програм “нотаріусів” для автентифікації цифрових сертифікатів, наданих серверами. Призначенням «нотаріусів» є збирання інформації щодо сертифікатів різних користувачів, які мають доступ до певного домену, та наступним використанням цієї інформації для захисту від використання хибних сертифікатів. Це ускладнює задачу зловмисника нав’язати хибну інформацію та зменшує вірогідність атаки MITM. Такий підхід був використаний в MECAI (Mutually Endorsing CA infrastructure), де «нотаріуси» також були центрами видачі сертифікатів, з обмеженням, що центр сертифікації не може бути власним «нотаріусом» для своїх сертифікатів. Ця вимога реалізує заборону використання самопідписаних сертифікатів та зменшує ризики MITM-атак.

Іншими підходами є використання суверенних ключів, додаткового контролю сертифікатів, спеціального середовища EFF SLL, MonkeySphere, AKI, Crossbear, DoubleCheck, S-Links, DNSChain, PoliCert, DetecTor та ICSI-нотаріус, опис яких можна знайти в [53].

Підсумовуючи огляд сценаріїв 1 та 2 можна зазначити, що вони є реактивними, що потребує постійного моніторингу та виявлення відхилень або аномалій у центрах видачі сертифікатів та у виданих цифрових сертифікатах.

В такому сенсі, альтернативними рішеннями є превентивні і активні підходи. Одним з таких рішень є використання технології децентралізованого розповсюдження та управління ключами (технології блокчейн) для забезпечення цілісності та автентичності процедур ідентифікації та автентифікації як центрів видачі сертифікатів, так і самих сертифікатів відкритих ключів.

Сценарій 3

Цей підхід оснований на використанні децентралізованих ідентифікаторів DID (Decentralized Identifiers), які визначені специфікацією W3C (World Wide Web Consortium), та використовуються децентралізованою системою управління ключами (Decentralized Key Management Systems-DKMS). Створення DKMS стала альтернативою існуючим системам, яка забезпечує захист від атак на мобільні платформи, які постійно змінюють позицію та з'єднуються з різними базовими станціями, що створює загрози процедурам генерації та розповсюдження криптографічних ключів. Відомим прикладом застосування DKMS стала концепція Vehicular Decentralized Key Management System (VDKMS) для мереж Cellular Vehicular-to-Everything (V2X). В основі концепції VDKMS лежить принцип суверенної ідентичності Self-Sovereign Identity (SSI). Принцип SSI заключається в використанні набору відомостей про особу, якими вона може керувати, ділитися з будь-якими приватними особами або публічними сервісами, відкликати до них доступ у будь-який час за своїм бажанням. Для ідентифікації даних застосовують формат Decentralized Identifier (DID). Принцип суверенної ідентичності SSI використовують для ефективної системи керування ключами, що дозволяє подолати обмеження на впровадження DKMS для мобільних платформ, прикладом яких є мережі VANET (Vehicular Ad hoc NETworks) та системи зв'язку з динамічною топологією MANET.

Для реалізації цього завдання використовують архітектуру, яка включає рівень додатку, рівень децентралізованої системи керування ключами, рівень SSI та рівень контролю транзакцій. Ця архітектура також називається технологією розподіленого реєстру (distributed ledger technology – DLT). З метою зменшення ризиків з незначними витратами на обчислення запропоноване рішення базується на використанні мікрореєстрів (distributed micro ledger technology – DMLT). Застосування DMLT для створення DKMS дозволяє забезпечити захист від більшості класів MITM-атак.

Структура DKMS на основі технології DMLT

Реалізація концепції DKMS включає наступні складові:

мобільна платформа;

реєстратор;

сервіс-провайдер;

блокчейн-складова (мікрореєстр).

Для взаємодії компонентів VDKMS здійснюються етапи:

забезпечення (Provision);

реєстрація (Registration);

перевірка облікових даних (Credentials Verification);

авторизація (Authorization).

Варіант побудови інфраструктури PKI з урахуванням особливостей розглянутих класів MITM-атак та сценаріїв захисту

Розглянемо варіант альтернативної інфраструктури PKI, яка має змішану інфраструктуру, що складається з елементів класичної PKI інфраструктури та елементів розподіленого реєстру. На рис. 7 наведена запропонована модель побудови гібридної системи розповсюдження криптографічних ключів.

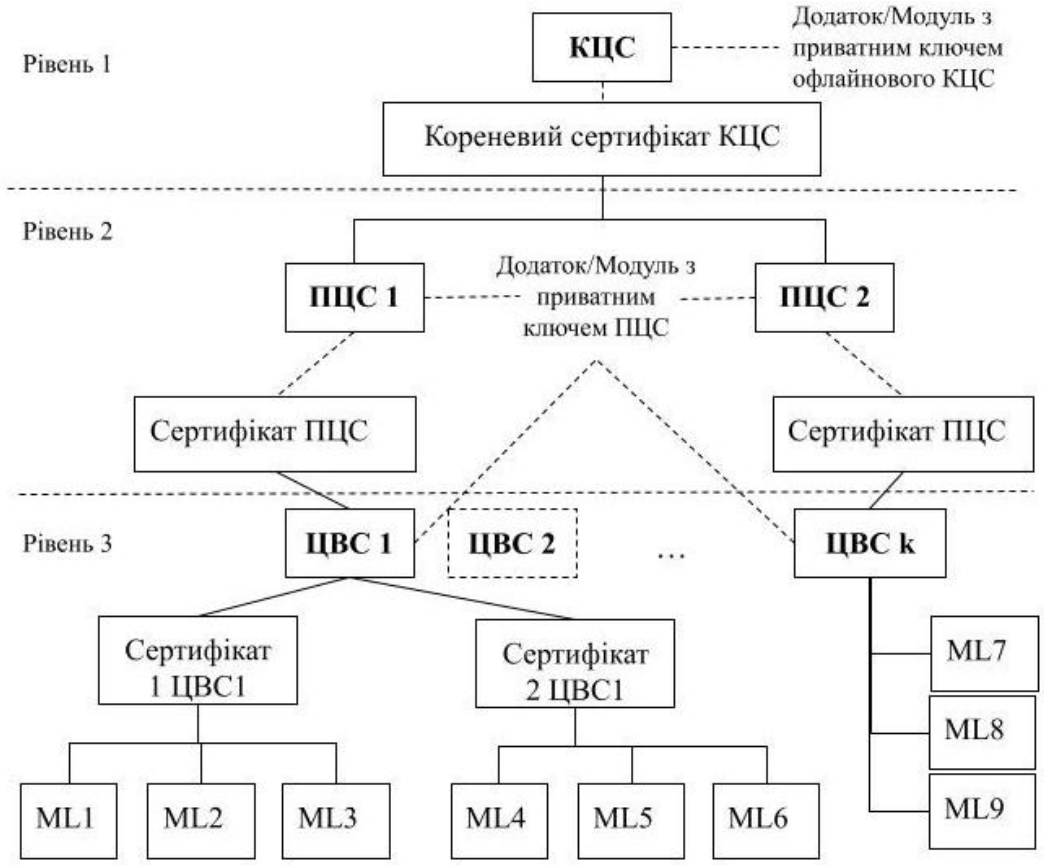

Рис. 7. Варіант альтернативної інфраструктури PKI з використанням концепції DKMS та технології DMLT

В запропонованій структурі розповсюдження криптографічних ключів на рис. 7 базовою структурою є існуюча модель побудови інфраструктури відкритих ключів, в якої на нижньому рівні, тобто на рівні, який найбільш схильний до впливів зловмисників, застосовується технологія розподілених мікрореєстрів (ML1-ML9), яка відрізняється від існуючої технології розподілених реєстрів використанням більш скороченого формату реєстру та підвищеною швидкістю транзакцій для обміну змінами реєстрів. Для побудови окремих ланцюгів (мікрореєстрів) використовуються сертифікати центрів видачі сертифікатів нижнього (третього рівня) (сертифікат 1 ЦВС 1, ЦВС 2, ЦВС k). В запропонованій схемі кожен реєстр є окремою мережею транзакцій, які можна розділяти як на окремі функціональні рівні, так і за рівнем критичності інформації, що планується оброблятися або передаватися в системі. Під час проведення експериментів були використані існуючі програмні бібліотеки для побудови блокчейну та створення мікрореєстрів [10, 11].

Висновки

В ході проведення дослідження було отримані результати аналізу існуючих способів організації атак "людина посередині" та способів реалізації кожного типу MITM-атак.

Визначено, що MITM-атаки є однією з найбільш небезпечних загроз практично усіх сучасних протоколів захисту інформації, що працюють через неконтрольовані канали передачі даних, а саме через безпровідні канали, через мережі стандарту 802.11 та через відкриті канали Інтернет. В якості об'єкта дослідження в роботі були визначені три варіанти побудови інфраструктури відкритих ключів, базова (однорівнева), дворівнева та багаторівнева. Визначені три класи центру розподілу криптографічних ключів, а саме: кореневий центр сертифікації ключів, центр видачі сертифікатів (ЦВС), проміжний центр сертифікації ключів. Визначено, вразливість (недолік) кожного підходу щодо побудови структурних схем взаємодії центрів сертифікації ключів, та обґрунтована перевага сегментування інфраструктури відкритих ключів з метою зниження шкоди під час компрометації або інших атак на інфраструктуру відкритих ключів.

Основним результатом, отриманим в роботі, є запропонована гібридна схема використання централізованого та децентралізованого підходу щодо розповсюдження криптографічних ключів, а саме використання класичної багаторівневої інфраструктури відкритих ключів, на нижньому рівні якої застосовується технологія децентралізованого розповсюдження ключів DKMS, яка використовує мікрореєстри, що зберігаються на кожному програмно-апаратному пристрої в клієнтському програмному забезпеченні. Запропоноване рішення дозволяє знизити ймовірність реалізації MITM-атаки на рівні доступу користувачів до центрів видачі сертифікатів пропорційно кількості користувачів для конкретного сегмента (окремого мікрореєстру). Також застосування технології DLT дозволить розділяти мережі на рівні сервісів, що надає можливість зменшити масштаби атак на інфраструктури та системи розповсюдження криптографічних ключів.

Наступним кроком досліджень заплановано дослідження показників швидкодії роботи розробленої гібридної інфраструктури з використанням технології DLT з використанням розробленого програмного забезпечення на основі відкритих джерел.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. A. Twigg, N. Dimmock. Attack-Resistance of Computational Trust Models. In Proceedings of the 12th IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE'03). 2003.

2. E. Bruneton, T. Coupaye, M. Leclerc, V. Quéma, and J.-B. Stéfani. The Fractal Component Model and its Support in Java. Software - Practice and Experience (SP&E), special issue on Experiences with Auto-adaptive and Reconfigurable Systems, 36 (11-12): 1257–1284, 2006.

3. A. Joseph Ed. "Security and Privacy in Pervasive Computing", IEEE Pervasive Computing, 6 (4): 73–75. 2007.

4. R. Oppliger, G. Pernul and C. Strauss, Using Attribute Certificates to Implement Role Based Authorization and Access Control Models, in the Proc. of 4. Fachtagung Sicherheit in Informationsystemen (SIS 2000), Zurich, Switzerland, 2000, 169–184.

5. G. Myles, A. Friday and N. Davies. Preserving Privacy in Environments with Location-Based Applications. Pervasive Computing, 2 (1): 56–64. 2003.

6. T. Dierks and C. Allen, The TLS Protocol Version 1.0, IETF RFC 2246, Jan. 1999.

7. Nicolas Serrano, Hilda Hadan, L. Jean Camp. A Complete Study of P.K.I. (PKI's Known Incidents) A. SSRN Electronic Journal · January 2019. Web: https://www.researchgate.net/publication/334789185.

8. URL: https://gist.github.com/ArturT/bc8836d3bedff801dc324ac959050d12.

9. URL: https://stackoverflow.com/questions/31621118/disable-sslv3-on-nginx.

10. URL: https://github.com/tko22/simple-blockchain.

11. URL: https://github.com/codingtmd/mini-blockchain/tree/master.