УДК 004.031

Сергій ТЕЛЕНЬКО, Сергій КУЛИНА

Західноукраїнський національний університет

СИСТЕМИ ЗАХИСТУ ПРИВАТНИХ КЛЮЧІВ НА ОСНОВІ АПАРАТНИХ МОДУЛІВ БЕЗПЕКИ

Вступ. В основі сучасної цифрової безпеки лежить асиметрична криптографія, де приватні ключі є найбільш критичним активом будь-якої організації. Вони є "ключами до королівства", що засвідчують цифрові особистості, шифрують конфіденційні дані та авторизують транзакції високої цінності. Однак традиційне зберігання цих ключів у програмному забезпеченні - у файлах конфігурації, базах даних або навіть в оперативній пам'яті сервера - робить їх надзвичайно вразливими. У разі компрометації сервера через зловмисне програмне забезпечення, мережеву атаку або інсайдерську загрозу, ці ключі можуть бути викрадені, що призводить до катастрофічних наслідків: повної втрати довіри, фінансових збитків та незворотної шкоди репутації.

Саме для вирішення цієї фундаментальної проблеми були створені апаратні модулі безпеки (Hardware Security Modules, HSM). Це спеціалізовані, захищені від фізичного втручання (tamper-resistant) пристрої, єдиною метою яких є безпечна генерація, зберігання та управління криптографічними ключами протягом усього їхнього життєвого циклу. Ключова перевага HSM полягає в тому, що приватні ключі ніколи не залишають захищеного апаратного периметра: всі криптографічні операції (наприклад, підписання або розшифрування) відбуваються безпосередньо всередині модуля. Таким чином, навіть якщо основний сервер, до якого підключений HSM, буде повністю скомпрометований, зловмисник не зможе викрасти сам приватний ключ, а отримає лише доступ до обмеженого набору функцій, що значно підвищує загальний рівень захищеності системи..

Метою дослідження є підвищення рівня безпеки та ефективності систем захисту приватних ключів шляхом розробки або вдосконалення методів їх інтеграції та управління на базі апаратних модулів безпеки (HSM).

1. Дослідження існуючих систем захисту приватних ключів на основі апаратних модулів безпеки

Системи захисту приватних ключів на основі апаратних модулів безпеки (HSM) є золотим стандартом для захисту найбільш критичних криптографічних активів в інфраструктурі будь-якої сучасної організації.

В основі цієї технології лежить принцип що приватні ключі ніколи не повинні залишати захищене апаратне середовище. У той час як програмні методи зберігають ключі у файлах, базах даних або пам'яті, що робить їх вразливими до викрадення через віруси, мережеві атаки або помилки конфігурації, HSM створює фізично та логічно ізольовану "чорну скриньку".

HSM - це спеціалізований обчислювальний пристрій, розроблений із захистом від несанкціонованого доступу. Його основні завдання - це безпечна генерація ключів, із використанням апаратного генератора випадкових чисел, захищене зберігання та суворий контроль над їхнім використанням. Коли

програмі або серверу потрібно виконати операцію з приватним ключем (наприклад, підписати документ, розшифрувати дані або випустити сертифікат), він надсилає запит до HSM. Модуль виконує операцію всередині свого захищеного криптографічного периметра і повертає лише результат, але не сам ключ. Навіть якщо зловмисник отримає повний контроль над сервером, він не зможе витягти ключ з апаратного модуля, оскільки він завжди біля власника (рисунок 1).

Рисунок 1 – Апаратний ключ доступу у вигляді брелка до ключів

Такі системи є життєво необхідними для інфраструктур Центрів сертифікації, де HSM захищає кореневий ключ, компрометація якого зруйнує всю систему довіри. Вони також є невід'ємною частиною банківських платіжних систем для захисту PIN-кодів та ключів транзакцій, підписання коду (для гарантії автентичності програмного забезпечення), шифрування баз даних (захист головного ключа шифрування) та блокчейн-додатків, захист ключів "гарячих" гаманців. Використання HSM кардинально підвищує стійкість системи до атак, забезпечуючи найвищий рівень гарантії, що приватні ключі залишаються справді приватними.

2. Типова структура системи захисту приватних ключів на основі HSM

Структура системи захисту приватних ключів на основі HSM є багаторівневою і поєднує програмні, апаратні та процедурні компоненти. Її типова архітектура, від "споживача" до "ядра" містить 5 рівнів:

1. Рівень застосунків (Споживачі). Бізнес-додатки, які нічого не знають про те, де знаходиться ключ, але знають, що їм потрібна криптографічна операція. Це можуть бути:

– Веб-сервери наприклад, Nginx, Apache для SSL/TLS-операцій.

– Сервери застосунків наприклад, Java, .NET для підписання токенів (JWT).

– Інфраструктура PKI - Центри сертифікації, для випуску сертифікатів.

– Бази данихтакі як Oracle, SQL Server для прозорого шифрування даних.

– Платіжні шлюзи для шифрування номерів карток.

2. Рівень абстракції (API та Клієнт HSM). Це "посередник" або "драйвер", який встановлюється на сервері застосунків. Він надає стандартизований інтерфейс для програм і "перекладає" їхні запити на мову, зрозумілу конкретному HSM.

3. Рівень підключення (Мережа або Шина). Це фізичний або логічний спосіб, у який сервери застосунків "спілкуються" з HSM. Найпоширенішим

варіантом є Мережевий HSM, якиц є окремим пристроєм у мережі (має свою IP-адресу). До нього можуть одночасно звертатися багато серверів. Зв'язок завжди захищений зашифрованим TLS-тунелем. Іншим поширеним вибором є вбудований HSM. Це карта, що вставляється безпосередньо в сервер, або USB-пристрій, який використовується коли потрібна максимальна продуктивність для одного конкретного сервера.

4. Апаратний Модуль Безпеки (HSM) - Ядро Системи. Це сам захищений пристрій, який має власну захищену операційну систему та апаратні компоненти.

Його внутрішня структура складається з:

– Захищений корпус, який має захист від несанкціонованого доступу. При спробі фізичного злому (наприклад, свердління) або зміни умов (температура, напруга) модуль автоматично знищує всі ключі.

– Криптографічний процесор – це спеціалізований чип, оптимізований для швидкого виконання асиметричних та симетричних операцій.

– Справжній генератор випадкових чисел (TRNG). Апаратний компонент для генерації криптографічно стійких ключів.

– Безпечне сховище ключів. Зашифрована енергонезалежна пам'ять, де ключі зберігаються у зашифрованому вигляді, а головний ключ, що шифрує всі інші, часто зберігається так, що його неможливо витягти.

– Захищена ОС та прошивка.

5. Рівень управління та аудиту - це процедури та інтерфейси, які використовуються для адміністрування самого HSM. Він містить безпечний канал управління - окремий, захищений інтерфейс (часто через SSH або захищений GUI) для налаштування політик, створення та видалення ключів.

Використання такої 5 рівневої структури дозволяє створити повнофункціональну систему, що відповідатиме поставленим задачам та забезпечить необхідний рівень надійності.

Висновок. З проведеного дослідження зрозуміло, що системи на основі апаратних модулів безпеки є не просто технічним доповненням, а фундаментальним рішенням однієї з найгостріших проблем кібербезпеки - захисту приватних ключів. Їхня ключова важливість полягає у створенні фізично ізольованого та захищеного від несанкціонованого доступу середовища, де криптографічні ключі генеруються, зберігаються та використовуються, але ніколи не залишають апаратного периметра. Як ми обговорили, така архітектура робить систему стійкою до програмних зломів, мережевих атак та навіть фізичного втручання. Таким чином, HSM є критичною інфраструктурною ланкою, що забезпечує найвищий рівень довіри та гарантій безпеки для важливих процесів, від функціонування центрів сертифікації до захисту фінансових транзакцій.

Перелік використаних джерел.

1. Sebestyen H., Popescu D. E., Zmaranda R. D. A Literature Review on Security in the Internet of Things: Identifying and Analysing Critical Categories. Computers. 2025. Vol. 14. № 2. Art. 61. DOI: 10.3390/computers14020061.

2. Khan, M., Ilyas, M., & Bayat, O. (2024, September). Enhancing IoT Security Through Hardware Security Modules (HSMs). In 2024 International Conference on Intelligent Computing, Communication, Networking and Services (ICCNS) pp.278-282.