УДК 681.3.06
DOI: 10.31673/2409-7292.2019.010615

Г.І. Гайдур, В.А. Козачок,
Р.М. Хмелевський, В.Є. Дмітрієв
https://orcid.org/0000-0003-0591-3290

ПІДВИЩЕННЯ ЗАХИЩЕНОСТІ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ ШЛЯХОМ ВИКОРИСТАННЯ TPM-МОДУЛІВ

В статті обґрунтована необхідність створення комплексних систем захисту інформації в інформаційно-телекомунікаційних системах, в яких обробляється інформація з обмеженим доступом. Розглянуті питання забезпечення збереження інформації, що накопичується в окремих файлах і базах даних. Розкриті основні принципи захисту ресурсних та фізичних об'єктів інформаційних систем. Показана необхідність використання прогресивних та перспективних технологій інформаційної безпеки.

Ключові слова: комплексна система захисту інформації, інформаційно-телекомунікаційна система, кріптопроцессор, довірена платформа, TPM-модуль.

Постановка проблеми.

Необхідність створення комплексних систем захисту інформації визначається законодавчими та нормативними вимогами [1, 2, 3].

Інформація, яка є власністю держави, або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, повинна оброблятися в системах із застосуванням комплексних систем захисту інформації.

Актуальність питання полягає в особливостях, які притаманні розподіленим інформаційно-телекомунікаційним системам, а саме: велика кількість споживачів; велика різноманітність вирішуємих завдань та наявність розгалужених зв'язків.

В даній статті обґрунтована необхідність використання TPM-модулів в якості прогресивної та перспективної технології інформаційної безпеки для підвищення рівня захищеності інформаційно-телекомунікаційних систем.

Виклад основного матеріалу.

У обчислювальній техніці TPM (Trusted Platform Module) – назва специфікації, що описує криптопроцессор, в якому зберігаються криптографічні ключі для захисту інформації, а також узагальнене найменування реалізацій вказаної специфікації, наприклад, у вигляді "чіпа TPM" або "облаштування безпеки TPM". Раніше він називався "Чіпом Фрица" (колишній сенатор Фриц Холлингс відомий своєю гарячою підтримкою системи захисту авторських прав на цифрову інформацію). Специфікація TPM розроблена організацією "Trusted Computing Group".

У січні 1999 року була створена робоча група виробничих компаній «Альянс довірюючих комп'ютерних платформ» (Trusted Computing Platform Alliance, TCPA) з метою розвитку механізмів безпеки і довіри в комп'ютерних платформах. Спочатку в TCPA входили провідні розробники апаратного та програмного забезпечення - HP, Compaq (в даний час підрозділ HP), IBM, Intel, Microsoft.

У жовтні 1999 року була анонсована проектна специфікація і відкрита можливість іншим компаніям приєднатися до альянсу. У серпні 2000 року була випущена для обговорення попередня публічна версія специфікації. Специфікація TCPA версії 1.0 була опублікована в лютому 2001 року, в ній були визначені основні вимоги до TPM з точки зору виробника електронних пристроїв. Потім була створена робоча група по створенню TPM, яка переглянула загальну специфікацію з точки зору практичного застосування довірюючого модуля. У серпні 2001 року була випущена специфікація версії 1.1 і створена робоча група з проектування платформи персональних комп'ютерів (ПК), на які встановлюється довірюючий модуль.

У квітні 2003 року була організована некомерційна організація «Trusted Computer Group» (TCG), яка стала наступником TCPA і продовжила працювати над розвитком вже випущених специфікацій. На додаток до вже створених робочих груп з проектування TPM і

платформи ПК були створені групи з розробки специфікацій для мобільних пристроїв, ПК-клієнтів, серверів, запам'ятовуючих пристроїв, інфраструктури довіряючих обчислень, програмного забезпечення (Trusted Software Stack, TSS) і довіряючого мережевого з'єднання. У листопаді 2003 року була опублікована специфікація TPM версії 1.2, остання версія з істотними змінами, в якій по суті описана функціональність TPM.

Trusted Platform Module (TPM), що містить в собі кріптопроцессор, забезпечує засоби безпечного створення ключів шифрування, здатних обмежити використання ключів (як для підпису, так і для шифрування/дешифрування) з тим же ступенем повторюваності, що і генератор випадкових чисел. Також цей модуль має наступні можливості: віддалену атестацію, прив'язку і надійне захищене зберігання. Віддалена атестація створює зв'язок апаратних засобів, завантаження системи і конфігурації хоста (операційної системи комп'ютера), дозволяючи третій особі перевіряти, щоб в програмне забезпечення не було внесено жодних змін. Кріптопроцессор шифрує дані таким способом, що вони можуть бути розшифровані тільки на комп'ютері, де були зашифровані, під керуванням того ж самого програмного забезпечення. Прив'язка шифрує дані, використовуючи ключ підтвердження - TPM-унікальний ключ RSA, записаний в чіп в процесі його виробництва, або інший ключ, якому довіряють.

Найефективнішим способом захисту системи, що виключає можливість проникнення хакерів, є використання апаратного чіпа TPM. Він являє собою невеликий «комп'ютер в комп'ютері»: довіряючий модуль з власним процесором, оперативною пам'яттю, накопичувачем і інтерфейсом вводу/виводу.

Головним завданням TPM є надання в розпорядження операційної системи гарантовано безпечних служб. Наприклад, чіпи TPM зберігають кріптоключи, що використовуються для шифрування даних на жорсткому диску. Крім того, модуль підтверджує ідентичність всієї платформи і перевіряє систему на можливі втручання хакерів в роботу апаратних засобів. На практиці TPM в тандемі з UEFI Secure Boot забезпечує користувачеві повністю захищений і безпечний процес запуску операційної системи.

Модуль TPM може використовуватися щоб підтвердити справжність апаратних засобів. Так як кожен чіп TPM унікальний для специфічного пристрою, це робить можливим однозначне встановлення автентичності платформи. Наприклад, щоб перевірити, що система, до якої здійснюється доступ - очікувана система.

Архітектура TPM [4].

Архітектура TPM-модуля наведена на рис. 1.

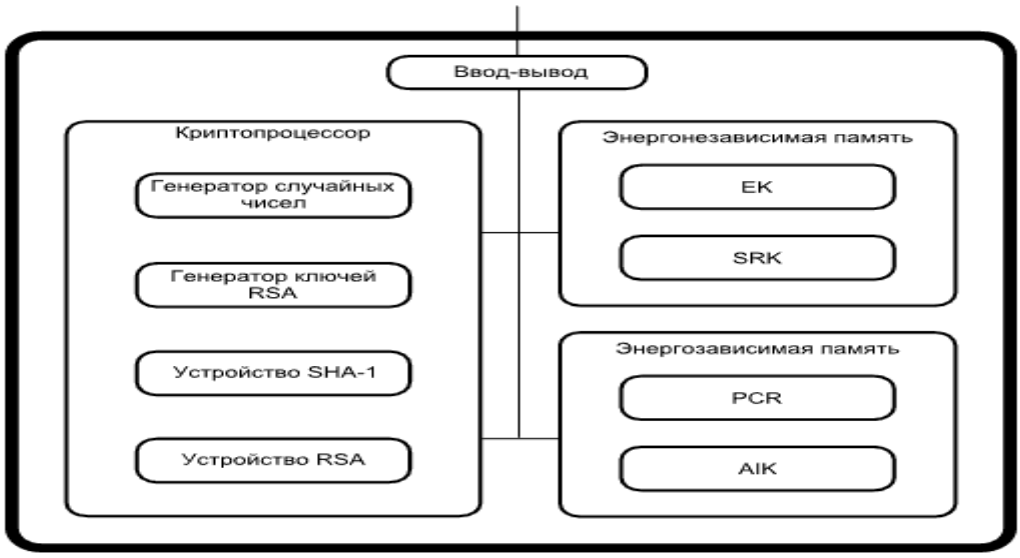

Рис. 1. Архітектура TPM-модуля

У специфікації TCG описаний мінімальний набір алгоритмів і протоколів, яким повинен задовольняти чіп TPM. Крім того, виробником можуть бути реалізовані додаткові алгоритми і протоколи (які, зрозуміло, повинні бути описані виробником у відповідній документації). В архітектурі чіпа реалізовані такі захисні механізми:

- захищене управління пам'яттю;
- шифрування шини і даних;
- тестування режимів блокування;
- активне екранування.

У чіп імплементовані алгоритми асиметричної криптографії, які забезпечують високий рівень захисту. Деякі елементи логічного дизайну чіпа є нестандартними з точки зору типових методів проектування інтегральних схем (IC). Застосовуються і спеціальні прийоми проектування IC: "заплутування" топології шарів IC, що ускладнює аналіз функцій елементів мікросхеми. Ряд технологічних особливостей чіпів безпеки спеціально не розголошується компаніями-виробниками, щоб зменшити ймовірність їх злому навіть в тому випадку, коли для цього застосовуються сучасні методи аналізу функціонування мікросхем і дороге устаткування.

Розглянемо більш детальніше елементи архітектури TPM-модуля.

Введення/Виведення (I/O). Цей компонент управляє потоком інформації по шині і управляє повідомленнями між відповідним компонентами TPM. I/O компонент вводить в дію політику доступу, пов'язану з функціями TPM. Правила доступу визначаються прапорами доступу, що зберігаються в блоці Opt-In незалежній пам'яті.

Криптографічний процесор. Здійснює криптографічні операції всередині TPM. Ці операції включають в себе:

- генерація асиметричних ключів (RSA);
- асиметричне шифрування/розшифрування (RSA);
- хешування (SHA-1);
- генерація випадкових чисел.

TPM використовує ці можливості для генерації випадкових послідовностей, генерації асиметричних ключів, цифрового підпису та конфіденційності даних, що зберігаються. Також TPM підтримує симетричне шифрування для внутрішніх потреб. Всі збережені ключі по складності повинні відповідати ключу RSA довжиною 2048 біт.

Незалежна пам'ять (Non-Volatile Storage). Використовується для зберігання ключа підтвердження, кореневого ключа (Storage Root Key, SRK), авторизаційних даних, різних прапорів доступу і блоку Opt-In. Обсяг цього типу пам'яті обмежений (1280 байт).

Ключ підтвердження (Endorsement Key, EK). EK-ключ RSA розміром 2048 біт, що ідентифікує чіп, а також весь пристрій, фундаментальний компонент TPM. Відкрита частина називається PUBEK, закрита - PRIVEK. Відповідно до політики безпеки PRIVEK не повинен бути доступний поза чіпом, він ніколи не використовується для генерування підписів. PUBEK зберігається в сертифікаті, використовується тільки для встановлення власника TPM і в процесі генерації AIK. EK генерується до того, як кінцевий користувач отримає платформу. Стандарт дозволяє змінити цей ключ, через що використання TPM може бути обмеженим.

Ключі підтвердження справжності (Attestation Identity Keys, AIK). AIK - ключ RSA довжиною 2048 біт, що використовується тільки для підписів, для шифрування не використовується. TPM може згенерувати необмежену кількість AIK, ці ключі повинні бути постійними, але рекомендується зберігати AIK в постійній зовнішньої пам'яті, а не всередині незалежній пам'яті TPM. Відповідно до специфікації передбачається, що виробники забезпечать достатньо місця для багатьох AIK, які будуть одночасно завантажуватися в енергозалежну пам'ять TPM. Перехід AIK від одного TPM до іншого заборонений.

Регістри конфігурації платформи (Platform Configuration Registers, PCR). PCR - це унікальні ознаки TPM, в яких в зашифрованому вигляді міститься вся інформація про

цілісність метрик системи, починаючи з завантаження BIOS до завершення роботи системи. Інформація, що міститься в PCR, формує корінь довіри для вимірювань (RTM), які можуть зберігатися як в незалежній, так і в енергозалежній пам'яті. Ці регістри скидаються при старті і при перезавантаженні системи. Специфікація визначає мінімальну кількість регістрів (16), кожен регістр містить 160 біт інформації. Регістри 0-7 зарезервовані для потреб TPM. Регістри 8-15 доступні для використання операційною системою і додатками. Зміни значень PCR незворотні і їх значення не можна записати безпосередньо, їх можна тільки розширити новими значеннями, які залежать від попередніх.

Генератор випадкових чисел (англ. Random Number Generator, RNG) використовується для генерації ключів і випадковостей в сигнатури (підписах). TPM повинен бути здатним забезпечити 32 випадкових біта на кожен виклик. RNG чіпа складається з наступних компонентів:

• джерело ентропії і колектор. Джерело ентропії - процес (або процеси), що забезпечують ентропію. Такими джерелами можуть бути шум, лічильник тактів процесора і інші події. Колектор ентропії - процес, який збирає ентропію, видаляє зміщення, вирівнює вихідні дані. Ентропія повинна передаватися тільки регістру стану;

• регістр стану. Реалізація регістра стану може використовувати 2 регістра: енергозалежної і незалежної пам'яті. При старті TPM завантажує енергозалежний регістр з енергонезалежного. При будь-якої змозі змінити регістр стану від джерела ентропії або від змішуючої функції, це впливає на енергозалежний регістр. При виключенні TPM записує поточне значення регістра стану в енергонезалежний регістр (таке оновлення може відбуватися і в будь-який інший час). Причиною такої реалізації є прагнення реалізувати незалежний регістр на флеш-пам'яті, кількість записів в яку обмежено. TPM повинен забезпечити відсутність експорту регістра стану;

• змішуюча функція бере значення з регістра стану і видає вихідні дані RNG. Кожне використання змішуючої функції повинно змінювати регістр стану. При втраті живлення відбувається скидання RNG. Будь-які вихідні дані RNG для TPM повинні бути захищені.

Блок SHA-1 (SHA-1 Engine) використовується для обчислення сигнатур (підписів), створення блоків ключів і інших цілей загального призначення. Хеш-інтерфейси доступні поза TPM. Це дозволяє оточенню мати доступ до хеш-функції.

Генератор ключів RSA (RSA Key Generator) створює пари ключів RSA. TCG не визначає вимог до часу генерації ключів.

Пристрій RSA (RSA Engine) використовується для цифрових підписів і шифрування. Немає обмежень на реалізацію алгоритму RSA. Мінімально рекомендована довжина ключа - 2048 біт. Виробники можуть використовувати китайську теорему про залишки або будь-який інший метод. Значення відкритої експоненти має бути 216+1.

Компонент Opt-In відповідає за стан TPM і статус володіння користувачем TPM. За це відповідають три групи змінних:

- TPM ввимкнено/вимкнено (в відключеному стані всі операції блокуються);
- TPM активований/деактивований (в деактивованому стані можливе виконання операцій, напр. Зміна власника);
- користувач пройшов/не пройшов аутентифікацію як власник модуля. Дана інформація зберігається у вигляді прапорів.

Ідея довіреної платформи або платформи, якій можна довіряти (її очікувана поведінка завжди збігається з реальною), заснована на понятті «корінь довіри» (Root of Trust) - набір компонентів, яким потрібно довіряти. Повний набір коренів довіри має мінімальну функціональність, необхідну для опису платформи, що впливає на доручення цій платформі. Є три кореня довіри: корінь довіри для вимірювань (RTM), корінь довіри для зберігання (RTS) і корінь довіри для повідомлень (RTR). RTM - обчислювальний механізм, який виробляє надійні вимірювання цілісності платформи. RTS - обчислювальний механізм, здатний зберігати хеши значень цілісності. RTR - механізм, який надійно повідомляє про

збереження в RTS інформації. Дані вимірювань описують властивості і характеристики вимірюваних компонентів. Хеши цих вимірів - «знімок» стану комп'ютера. Їх зберігання здійснюється функціональністю RTS і RTR. Порівнюючи хеш виміряних значень з хешом довіреного стану платформи, можна судити про цілісність системи.

Приклади можливого застосування TPM-модулів. [5].

Аутентифікація. TPM є токен аутентифікації наступного покоління. Кріптопроцессор підтримує аутентифікацію як користувача, так і комп'ютера, забезпечуючи доступ до мережі тільки авторизованим користувачам і комп'ютерам. Це може використовуватися, наприклад, при захисті електронної пошти, заснованої на шифруванні або при підписах цифрових сертифікатів, прив'язаних до TPM. Відмова від паролів і використання TPM дозволяють створити більш потужні моделі аутентифікації для проводового, бездротового і VPN доступу.

Захист даних від крадіжки. Це є основним призначенням «захищеного контейнера». Самошифруючи пристрої, реалізовані на основі специфікацій (Trusted Computing Group), роблять доступними вбудоване шифрування і контроль доступу до даних. Такі пристрої забезпечують повне шифрування диска, захищаючи дані при втраті або крадіжці комп'ютера.

Переваги:

• Покращення продуктивності. Апаратне шифрування дозволяє оперувати з усім діапазоном даних без втрат продуктивності.

• Посилення безпеки. Шифрування завжди включено. Крім того, ключі генеруються всередині пристрою і ніколи не покидають його.

• Низькі витрати використання. Не потрібні модифікації операційної системи, додатків і т. ін. Для шифрування не використовуються ресурси центрального процесора. Великі перспективи має зв'язка TPM+Bitlocker. Таке рішення дозволяє прозоро від ПЗ шифрувати весь диск.

Управління доступом до мережі (NAC). TPM може підтверджувати справжність комп'ютера і навіть його працездатність ще до отримання доступу до мережі і, якщо необхідно, поміщати комп'ютер в карантин.

Захист ПЗ від зміни. Сертифікація програмного коду забезпечить захист ігор від читерства, а програм, що вимагають особливої обережності, наприклад банківських і поштових клієнтів - від навмисної модифікації. Відразу ж буде припинено додавання «троянського коня» в додатках, які встановлюються.

Захист від копіювання. Захист від копіювання заснований на такому ланцюжку: програма має сертифікат, що забезпечує їй (і тільки їй) доступ до ключа розшифрування (який також зберігається в TPM). Це дає захист від копіювання, який неможливо обійти програмними засобами.

Приклади реалізація TPM-модулів [5, 6].

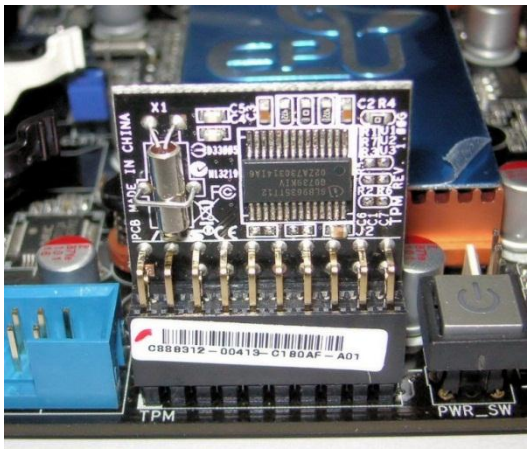

Рис. 2. TPM-модуль Infineon на материнській платі Asus P5Q PREMIUM

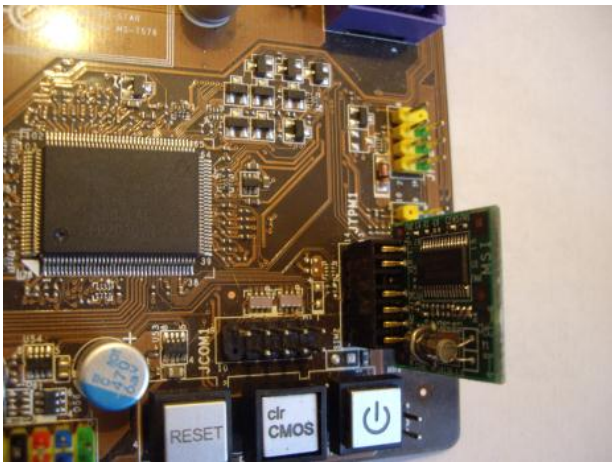

Рис. 3. TPM-модуль на материнській платі Intel

Хоча специфікація передбачає як апаратну, так і програмну реалізації системи TPM, забезпечення належного рівня безпеки, встановленого в загальній специфікації, на сьогоднішній день можливо тільки при апаратній реалізації. Апаратна реалізація у вигляді чіпа TPM була вперше випущена в 2005 році. На сьогоднішній день чіпом TPM оснащено більше 500 000 000 комп'ютерів. В майбутньому TPM зможе встановлюватися на такі пристрої, як мобільні телефони, пристрої введення і зберігання інформації. Мікроконтролери TPM на сьогоднішній день розробляються і застосовуються багатьма компаніями.

Критика TPM-модулів. [6].

Проблема «довіри». Trusted Platform Module критикується деякими IT-фахівцями за назву. Довіра (Trust) завжди має бути обоюдною, в той час як розробники TPM користувачеві не довіряють, що призводить до обмеження свободи. На думку окремих IT-фахівців, для довірених обчислень більше підходить назва «віроломні обчислення» (Treacherous computing), оскільки наявність модуля гарантує зворотне - систематичний вихід комп'ютера з підпорядкування. Фактично, комп'ютер перестає функціонувати як комп'ютер загального призначення, оскільки будь-яка операція може зажадати явного дозволу власника комп'ютера.

Втрата «володіння» комп'ютером. Власник комп'ютера більше не може робити з ним все, що завгодно, оскільки передає частину своїх прав виробникам програмного забезпечення. Зокрема, TPM може заважати (через помилки в ПЗ або навмисного рішення розробників):

- переносити дані на інший комп'ютер;
- вільно вибирати програмне забезпечення для свого комп'ютера;
- обробляти наявні дані будь-якими доступними програмами.

Втрата анонімності. Комп'ютер, обладнаний TPM, має унікальний ідентифікатор, зашитий в чіпі. Ідентифікатор відомий виробнику програмного забезпечення і його неможливо змінити. Це ставить під загрозу одне з природних переваг Інтернету - анонімність. На даний момент, якщо на комп'ютері немає троянських програм, в програмному забезпеченні немає явних помилок, а cookie видалені, єдиним ідентифікатором користувача залишається IP-адреса і заголовки HTTP. Поряд з підвищенням безпеки, наявність модуля TPM може мати негативний ефект на свободу слова, що особливо актуально для країн, що розвиваються. Щоб зрозуміти, до чого може привести віддалено читаємий і незмінний ідентифікатор комп'ютера, досить згадати аналогічну проблему з ідентифікаційним номером процесора Pentium III.

Потенційна загроза вільної конкуренції. Програма, яка стала лідером галузі (як AutoCAD, Microsoft Word або Adobe Photoshop), може встановити шифрування на свої

файли, унеможливлюючи доступ до цих файлів за допомогою програм інших виробників, створюючи, таким чином, потенційну загрозу вільної конкуренції на ринку прикладного ПЗ.

Проблеми несправності модуля TPM. У разі несправності модуля TPM - контейнери, захищені їм, стають недоступними, а дані, що знаходяться в них - невідновними. Для повної гарантії відновлення даних у разі псування модуля TPM необхідно здійснювати складну процедуру резервного копіювання. Для забезпечення секретності система резервного копіювання (backup) також повинна мати власні TPM-модулі.

Зломи. На конференції з комп'ютерної безпеки Black Hat 2010 року було оголошено про злом чіпа Infineon SLE66 CL PE, виготовленого за специфікацією TPM. Даний чіп використовується в комп'ютерах, обладнанні супутникового зв'язку і ігрових приставках. Для злому використовувався електронний мікроскоп (вартістю близько $ 70 000). Оболонка чіпа була розчинена кислотою, для перехоплення команд були використані найдрібніші голки. У Infineon стверджують, що вони знали про можливість фізичного злому чіпа. Борчерт, віце-президент компанії, запевнив, що дороге обладнання і технічна складність злому не представляє небезпеки для переважної більшості користувачів чіпів.

Рекомендації по використанню довіреного платформеного модулю. [6, 7].

Порівняння TPM версії 1.2 і 2.0. Корпорація Microsoft є лідером у галузі по стандартизації модуля TPM 2.0 і переходу на його використання. TPM 2.0 містить багато реалізованих переваг, пов'язаних з алгоритмами, шифруванням, ієрархією, кореневими ключами, авторизацією і незалежною оперативною пам'яттю.

Переваги TPM 2.0. Продукти й системи на основі TPM 2.0 мають важливі переваги безпеки в порівнянні TPM 1.2, в тому числі:

• Специфікації TPM 1.2 дозволяють використовувати тільки RSA і алгоритм хешування SHA-1.

• З метою безпеки деякі організації перестають використовувати SHA-1. Зокрема, Національний інститут стандартів і технологій США (NIST) зажадав від багатьох федеральних агентств перейти на використання SHA-256, починаючи з 2014 року, а технологічні лідери, включаючи Майкрософт і Google, оголосили про припинення з 2017 року підтримки підпису і сертифікатів на основі SHA-1.

• TPM 2.0 підтримує велику криптографічну гнучкість, так як дозволяє більш гнучко працювати з криптографічними алгоритмами.

• TPM 2.0 підтримує SHA-256, а також ECC, причому ECC є критично важливим для підвищення продуктивності створення ключів і підпису.

• TPM 2.0 отримав стандартизацію ISO (ISO/ IEC 11889: 2015).

• Використання TPM 2.0 допоможе виключити необхідність внесення виробниками обладнання винятків в стандартні конфігурації для продажу пристроїв в деяких країнах і регіонах.

• TPM 2.0 надає більш узгоджену взаємодію при всій різноманітності впровадження.

• Реалізації TPM 1.2 як в дискретному вигляді, так і у вбудованому ПЗ, розрізняються за параметрами політики. Це може привести до проблем з технічною підтримкою у зв'язку з відмінностями політик блокування.

• Вимога до стандартизації політики TPM 2.0 дозволяє встановити узгоджену поведінку блокування на різних пристроях, тому Windows може забезпечити більш якісну взаємодію з користувачами на всіх етапах.

• Тоді як деталі TPM 1.2 представляли собою дискретні кремнієві компоненти, припаяні до системної плати, TPM 2.0 доступна як у вигляді дискретного (dTPM) кремнієвого компонента, так і у вигляді компонента на основі вбудованого ПЗ (fTPM), який працює в довіреному середовищі виконання (TEE) в основній системі на кристалі (SoC):

• На мікросхемах Intel, це Intel Management Engine (ME) або Converged Security Engine (CSE);

• На мікросхемах AMD, це AMD Security Processor;

• На мікросхемах ARM, це Trustzone Trusted Application (TA).

Якщо TPM використовується в якості вбудованого ПЗ для настільних систем Windows, постачальник мікросхем надає виробникам відповідного обладнання реалізацію вбудованого ПЗ TPM разом з іншим вбудованим ПЗ на мікросхемі.

Дискретний TPM або TPM у вигляді вбудованого ПЗ?

Windows використовує дискретний TPM і TPM у вигляді вбудованого ПЗ однаково. При використанні будь-якого з цих варіантів для Windows немає ніяких функціональних переваг або недоліків.

З точки зору безпеки дискретний TPM і TPM у вигляді вбудованого ПЗ мають однакові характеристики:

• обидва варіанти здійснюють безпечне виконання на основі обладнання;

• обидва варіанти використовують вбудоване ПЗ для деяких функціональних можливостей TPM;

• обидва варіанти мають функції захисту від злому;

• обидва варіанти мають унікальні обмеження і ризики, пов'язані з безпекою.

Список літератури:

1. Закон України “Про захист інформації в інформаційно-телекомунікаційних системах” від 05.07.94 № 81/94ВР.

2. Постанова КМ України № 373 від 29.03.06 “Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах”.

3. ДСТУ 3396.1-96 Захист інформації. Технічний захист інформації. Порядок проведення робіт.

4. Microsoft corp. URL: https://technet.microsoft.com/ru-ru/library/mt604232(v=vs.85).aspx.

5. Alan M. Dunn, Owen S. Hofmann, Brent Waters, Emmett Witchel Cloaking Malware with the Trusted Platform Module // SEC'11 Proceedings of the 20th USENIX conference on Security. - USENIX Association, 2011.

6. Allan Tomlinson Introduction to the TPM // Smart Cards, Tokens, Security and Applications. - Springer, 2008. - С. 155-172. - DOI: 10.1007 / 978-0-387-72198-9_7.

7. Eimear Gallery, Chris J. Mitchell Trusted Computing: Security and Applications // Cryptologia. - Taylor & Francis, 2008. - Вип. 33. - С. 217-245. - DOI: 10.1080 / 01611190802231140.