НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені Ігоря СІКОРСЬКОГО»
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ

Кафедра математичних методів захисту інформації

ЛАБОРАТОРНА РОБОТА №4

на тему: "Дослідження особливостей реалізації існуючих програмних систем, які використовують криптографічні механізми захисту інформації"

Виконали: студенти 5 курсу, групи ФІ-12мп
Бублик Єгор, Волинський Євгеній та Слуцький Андрій

Київ — 2021

1. Мета роботи

Отримання практичних навичок побудови гібридних криптосистем.

2. Завдання на лабораторну роботу

Розробити реалізацію асиметричної криптосистеми (Ель-Гамаля під Windows платформу, на основі PyCrypto) у відповідності до стандартних вимог Crypto API або стандартів PKCS та дослідити стійкість стандартних криптопровайдерів до атак, що використовують недосконаліть механізмів захисту операційної системи.

3. Дослідження стійкості стандартних криптопровайдерів

Відразу хочеться зазначити, що знайти матеріали за даною темою дуже важко, оскільки Microsoft, для якої дуже важлива репутація, намагається приховати всі факти існування вразливостей власних продуктів та сервісів, тим більше тих, які використовуються у криптографічних цілях, і не тільки приватними особами.

Нам вдалося знайти роботу, в якій досліджуються вразливості стандартних криптопровайдерів Windows платформи, але є один нюанс — актуальність роботи датується роками використання Windows XP, тобто більше 10 років тому. З тих пір було зроблено безліч security-патчів, а підтримка Windows XP була завершена у 2014 році.

Що стосується актуальних версій ОС — жодної інформації знайдено не було.

Проте, потенційну загрозу криптопровайдерам можуть створювати Intel Management Engine Interface та її аналог, AMD Secure Technology — автономні підсистеми, вбудовані майже в усі чіпсети процесорів Intel та AMD відповідно. Вона складається з пропрієтарної прошивки, що виконується окремим мікропроцесором. Так як чіпсет завжди підключений до джерела струму, ця підсистема продовжує працювати, навіть коли комп'ютер вимкнено.

Через вказані підсистеми проходить весь «трафік», який існує на комп'ютері, в тому числі, можливо, ключі, отримані від криптопровайдерів. Існує експлойт **SA-00086**, тому практично кожен комп'ютер на базі Intel, випущений останні кілька років, вразливий і може бути скомпрометований, хоча шляхи використання вразливості точно не відомі. Аналогічна вразливість була знайдена у AMD Secure Technology в 2018 році, AMD підтвердила наявність проблеми та оголосила про доступність оновлень прошивки, після чого нових проблем з безпекою знайдено не було.

4. Висновки

Під час виконання лабораторної роботи, наша реалізація схеми шифрування та ЦП Ель-Гамаля була приведена до стандарту Crypto API: простір імен власного модуля приведений до зазначених у стандарті, кожен метод містить відповідний *docstring*, наведені описи аргументів, можливі помилки при використанні та коди повернення.

Також було проведено дослідження стійкості стандартних криптопровайдерів, розглянуті можливі атаки.

Під час виконання роботи ми набули навичок з практичної побудови гібридних криптосистем, розробки у відповідності до стандартів Crypto API та PKCS та дослідження стійкості стандартних криптопровайдерів.