Національний технічний університет України
«Київський політехнічний інститут»

Фізико технічний інститут

Кафедра математичних методів захисту інформації

МЕТОДИ РЕАЛІЗАЦІЇ КРИПТОГРАФІЧНИХ МЕХАНІЗМІВ

Лабораторна робота №4

Тема: “Дослідження особливостей реалізації існуючих програмних систем, які використовують криптографічні механізми захисту інформації.”

Виконали:
Драга Владислав ФІ-12мп
Чіхладзе Вахтанг ФІ-12мн

Перевірила
Селюх П.В.

Київ 2021

Мета роботи: Отримання практичних навичок побудови гібридних криптосистем.

Завдання:
Розробити реалізацію асиметричної криптосистеми у відповідності до стандартних вимог Crypto API або стандартів PKCS та дослідити стійкість стандартних криптопровайдерів до атак, що використовують недосконалість механізмів захисту операційної системи.
Дослідити бібліотеку PyCrypto під Linux платформу, за яким реалізовано криптографічний механізм цифрового підпису за стандартом ДСТУ 4145-2002.

Хід роботи

Для реалізації криптосистеми у відповідності до стандартних вимог Crypto API використаємо реалізовану в лабораторній роботі №3 систему цифрового підпису за стандартом ДСТУ 4145-2002. Для виконання цього завдання було написано клас обгортка, що викликає функції класу DSTU. А саме:
1. generate_private_key()
2. generate_public_key()
3. export_private_key()
4. export_public_key()
5. import_private_key()
6. import_public_key()
7. sign()
8. verify().
9. del_private_key()
10. del_public_key()

Як недолік операційної системи можна виділити генерацію випадкових чисел на основі ентропії. Відомо, що ентопія в Linux залежить від випадкових дій користувача. Якщо написати програму

емулятор користувача, та взяти під контроль ентропію, то можна впливати на генерацію ключів і з великою точністю робити прогноз щодо бітів ключа. Знаючи які біти в ключі, перебор ключів значно зменшується, а це впливає на стійкість криптосистеми.

Висновок: було досліджено один з векторів атак на генератор випадкових чисел, яким можно скомпрометувати генерацію ключів. Також було реалізовано клас обгортка над реалізованою криптосистемою з лабораторної роботи №3, що реалізує вимоги Crypto API.

Посилання:

1. https://blog.cr.yp.to/20140205-entropy.html