Как некорректное использование криптосредств может привести к уязвимостям в прикладных информационных системах

Алексеев Евгений Константинович,
начальник отдела криптографических исследований
ООО «КРИПТО-ПРО»

КРИПТОПРО

XI симпозиум
«Современные тенденции в криптографии»
CTCrypt 2022

В чем проблема?

- Требование о проведении оценки влияния при использовании СКЗИ
- Частые мнения и вопросы:
  - ✓ Мы же уже купили СКЗИ, что вам от нас еще нужно?
  - ✓ Какое же это СКЗИ, если нужны новые исследования при каждом встраивании?
- Далее рассмотрим примеры того, как некорректное использование СКЗИ может привести к возникновению уязвимостей в прикладных информационных системах

КРИПТОПРО

Архитектура безопасности информационных систем

Оценка влияния при встраивании СКЗИ:

- Проверка корректности условий использования СКЗИ
- Проверка корректности целей использования СКЗИ
- Проверка корректности программного кода
- Отсутствие негативного влияния среды функционирования
- …

КРИПТОПРО

Отсутствие необходимых проверок

- Отсутствие реальной проверки подписи
- Отсутствие проверок, связанных с PKI-инфраструктурой
- Нет проверок кодов возврата для вызовов датчика случайных чисел

3,216 code results Sort: Best match

will127534/HITCON-Badge-2018
Software/HitconBadge2018/util.cpp

```
102    uint32_t max = pow(10,digit);
103
104    hal_trng_get_generated_random_number(&number);
105    return number%max;
106  }
107
108  uint32_t randomUint32_t_generator(){
109    uint32_t number = 0;
110    hal_trng_get_generated_random_number(&number);
111    return number;
```

C++ Showing the top two matches Last indexed on Apr 14

36,696 code results Sort: Best match

NovasomIndustries/NFC_Reader
Core/Src/NFC_Reader/NFC_EncDec.c

```
52          for(j=0;j<16;j++)
53          {
54                  HAL_RNG_GenerateRandomNumber(&hrng, &random_number);
55                  host_buff[j*4]          = (random_number>>24) & 0xff;
            ...
67          for(j=0;j<4;j++)
68          {
69                  HAL_RNG_GenerateRandomNumber(&hrng, &random_number);
70                  buffer[j*4]             = (random_number>>24) & 0xff;
71                  buffer[(j*4)+1]         = (random_number>>16) & 0xff;
```

C Showing the top two matches Last indexed on May 7

https://bishopfox.com/blog/youre-doing-iot-rng

КРИПТОПРО

Повторное использование ключей

Ключ подписи используется для:

- аутентификации клиента при установлении соединения по протоколу TLS;
- для подписания электронных документов, циркулирующих в рамках системы.

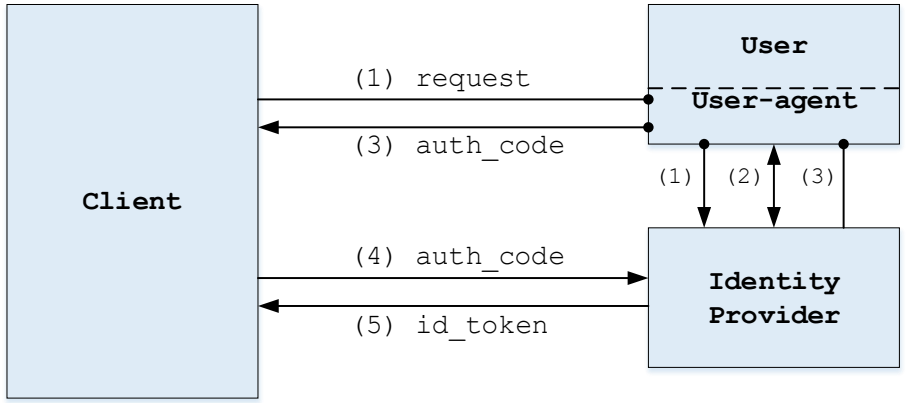
Уязвимость:

- Сервер в рамках аутентификации в TLS формирует данные для подписания клиентом так, что по содержанию они совпадают с некоторым документом

Некорректная оценка целевых свойств

Протокол OpenID Connect:

- предназначен для «делегированной» идентификации и аутентификации пользователей
- определен для интеграции с одним сервером идентификации (Identity Provider), но прозрачно расширяем на случай нескольких серверов



Базовая версия не является стойкой в случае, если один из серверов авторизации является нарушителем (возможна ложная аутентификация)

«On the security of modern Single Sign-On Protocols – Second-Order Vulnerabilities in OpenID Connect», 2016

КРИПТОПРО

Некорректное комбинирование функций СКЗИ

- Цель: необходимо обеспечить конфиденциальность и аутентификацию сообщения
- Решение: CMS SignedData + CMS EnvelopedData

1. Sign

SIGNATURE

2. Encrypt

3. Send

+ SIGNATURE

Некорректное комбинирование функций СКЗИ

- Уязвимость: если подписываются малоэнтропийные данные (например, неизвестна только сумма контракта), то по значению подписи можно восстановить эти данные (путем перебора, критерий – успешная проверка подписи)

+ SIGNATURE

Некорректное комбинирование функций СКЗИ

- Правильное решение: шифровать подпись вместе с документом

1. Sign

SIGNATURE

2. Encrypt

3. Send

Вопросы

Спасибо за внимание!
Вопросы?