

Мобильные устройства с выделенным криптографическим процессором

Введение

Рассмотрим две платформы, где **CryptoMCU** используется как отдельная микросхема и «общается» с основным **CPU** через внешнюю шину.

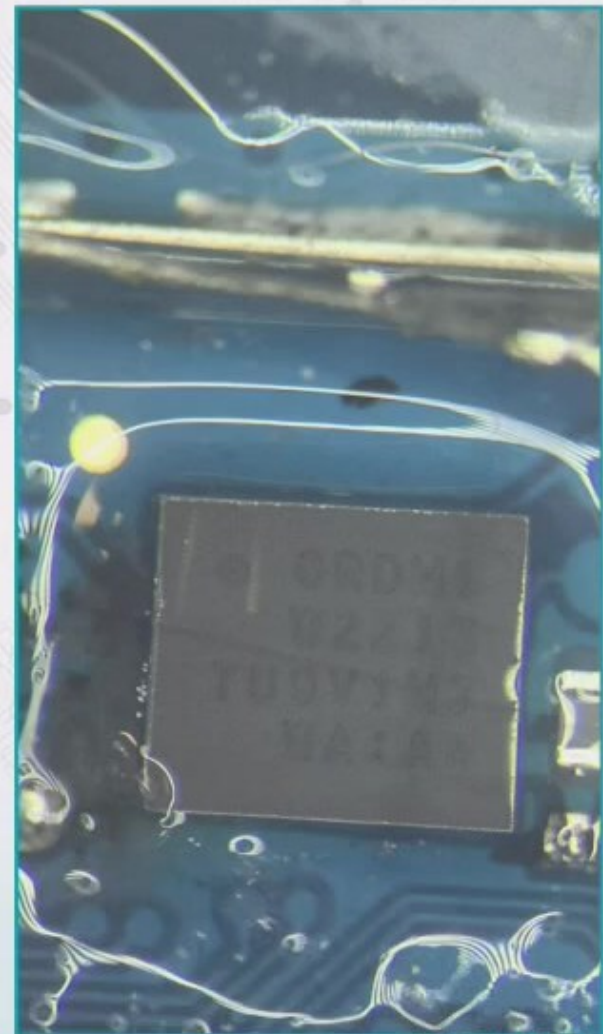
- **MTK и Unisoc**

Рассмотрим решения для этих устройств от SAMSUNG

- **Kirin / Exynos**

Задача ещё сложнее

Цель: понять, когда работу с паролем можно вынести за пределы телефона, а когда наличие CryptoMCU принципиально исключает такую возможность.



CryptoMCU

Устройства и интерфейсы

Samsung Galaxy TAB A8 SM-X205

CPU
Unisoc Tiger T618

CryptoMCU
S3FV9RRYDW-UK3A

Интерфейс: SPI

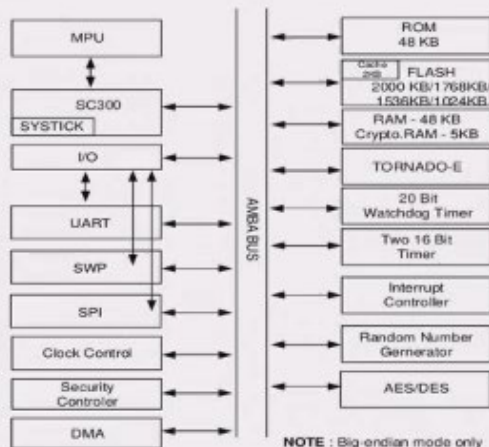
Samsung Galaxy A06 SM-A065

CPU
MTK Helio G85

CryptoMCU
S3K250AFDY-MF35

Интерфейс: I²C

S3FV9RRYDW-UK3A (S3FV9RR)



NOTE : Big-endian mode only

S3FV9RR eSE

Публичные характеристики S3FV9RR

Категория

eSE

Применения

Mobile, Lifestyle

Ядро

SC300 · 70 MHz

Flash / RAM

2000 KB / 53K

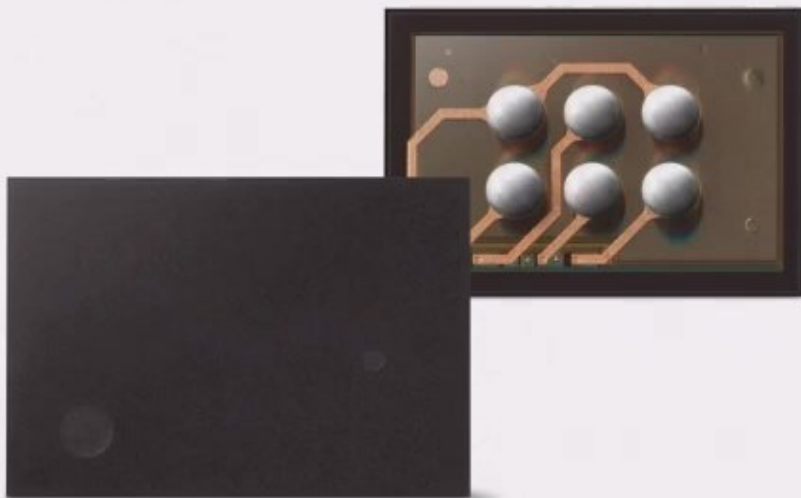
Crypto

DES · 3DES · AES · RSA · ECC · Tornado-E

Интерфейсы

SPI slave · SWP · GPIO

S3K250AFDY-MF35 (S3K250AF)



Samsung Secure Element S3K250AF

Публичные характеристики S3K250AF

Тип	Secure IC
Применения	Mobile, Lifestyle
Ядро	SC000
Память	Flash 252K · ROM 17K · RAM 11K
Скрипто	DES · 3DES · AES · RSA · ECC · TORNADO-T
Интерфейсы	ISO 7816 · I ² C

Galaxy TAB A8: схема сборки ключа

От cryptoMCU нужно получить блоб (knox_nonce). После его получения проверку пароля можно перенести из устройства.

knox_nonce + rot + color + is_locked + secdis
+ some_const + hw_unique + user_pwd

key_for_encrypted_key

fs_space_key

Galaxy TAB A8: доступ к CryptoMCU



SPI-мониторинг не раскрывает Knox_nonce — мешают Challenge и шифрованный обмен.

Почему пассивный SPI-мониторинг не решает задачу

Даже если физически подключиться к шине, это не эквивалентно получению knox_nonce.



Нужно не просто «видеть» транзакцию, а участвовать в ней как легитимная сторона или управлять ею через процессор устройства.

Как узнать knox_nonce: пассивные варианты

1. Смониторить SPI

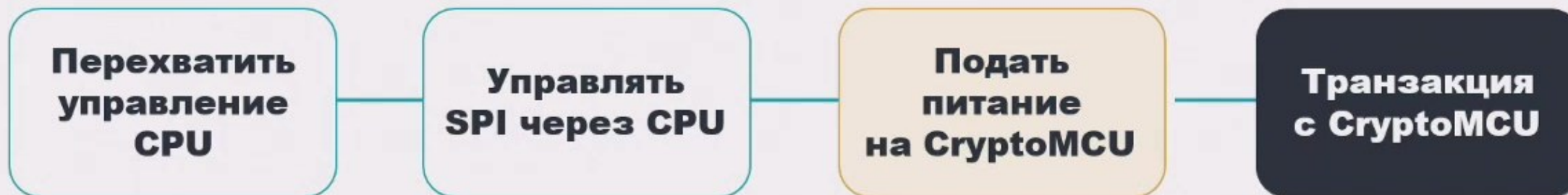
Не получается: Challenge и зашифрованный обмен не дают извлечь полезный knox_nonce из пассивного трафика.

2. Узнать ключ Challenge

Вариант с выпаиванием и чтением микросхемы выглядит лучше, но ключ завязан на процессор.

Вывод: нужен переход от наблюдения к управлению процессором устройства.

Как узнать `knox_nonce`: активный путь



Особая сложность: питание CryptoMCU включается только на время транзакций через отдельную систему защиты.

реализуемо, но сложно

ТАВ А8: промежуточный вывод

Сложность высокая

Challenge, secure channel, привязка ключа к процессору и управление питанием CryptoMCU создают аппаратный барьер.

Но результат переносим

Если knox_nonce получен, user_pwd участвует в алгоритме, который можно реализовать вне телефона.

Вывод: несмотря на сложность, эта схема допускает вынос перебора пароля пользователя из устройства.

Переход к Galaxy A6 / SM-A065



Ключевой момент: наличие Weaver переносит контроль аутентификации пользователя в CryptoMCU.

Почему результат не гарантирован

Если нужен только секретный
блоч

**получили блоч
+
проверяем user_pwd
снаружи**

логика TAB A8

Если проверка внутри CryptoMCU

**user_pwd
проверяется
через CryptoMCU**

логика Weaver

Weaver меняет модель защиты

CryptoMCU участвует в проверке и управляет попытками.

```
rot + color + is_locked + secdis + some_const  
+ hw_unique + user_pwd + weaver_info
```

hash

CryptoMCU

key_for_encrypted_key

fs_space_key

**пароль проверяется
внутри CryptoMCU**

**счётчик попыток
контролируется MCU**

**ошибки могут
фиксироваться**

Что именно меняет Weaver

1

Контроль auth в CryptoMCU

Проверка user_pwd не сводится к алгоритму, который может бесконечно работать вне устройства.

2

Счётчик попыток

CryptoMCU может ограничивать количество попыток и тем самым менять скорость перебора.

3

Фиксация ошибок

Неправильные попытки могут фиксироваться внутри устройства, в том числе устройство может перестать отвечать

Когда возможен внешний подбор

Где проверяется
user_pwd?

```
graph TD; Q[Где проверяется user_pwd?]; Q --> TOS[TOS/OS<br/>пример: TAB A8]; Q --> CryptoMCU[CryptoMCU<br/>пример: SM-A065];
```

TOS/OS
пример: TAB A8

внешний перебор возможен

CryptoMCU
пример: SM-A065

внешний перебор невозможен

**Спасибо
за внимание!**

