Преодоление парольной защиты и получение доступа к защищенным данным для некоторых моделей мобильных устройств Samsung в сложных случаях

Чиликов А.А., к.ф.-м.н., доцент кафедры «Информационная безопасность», МГТУ им.Баумана, Passware Inc.

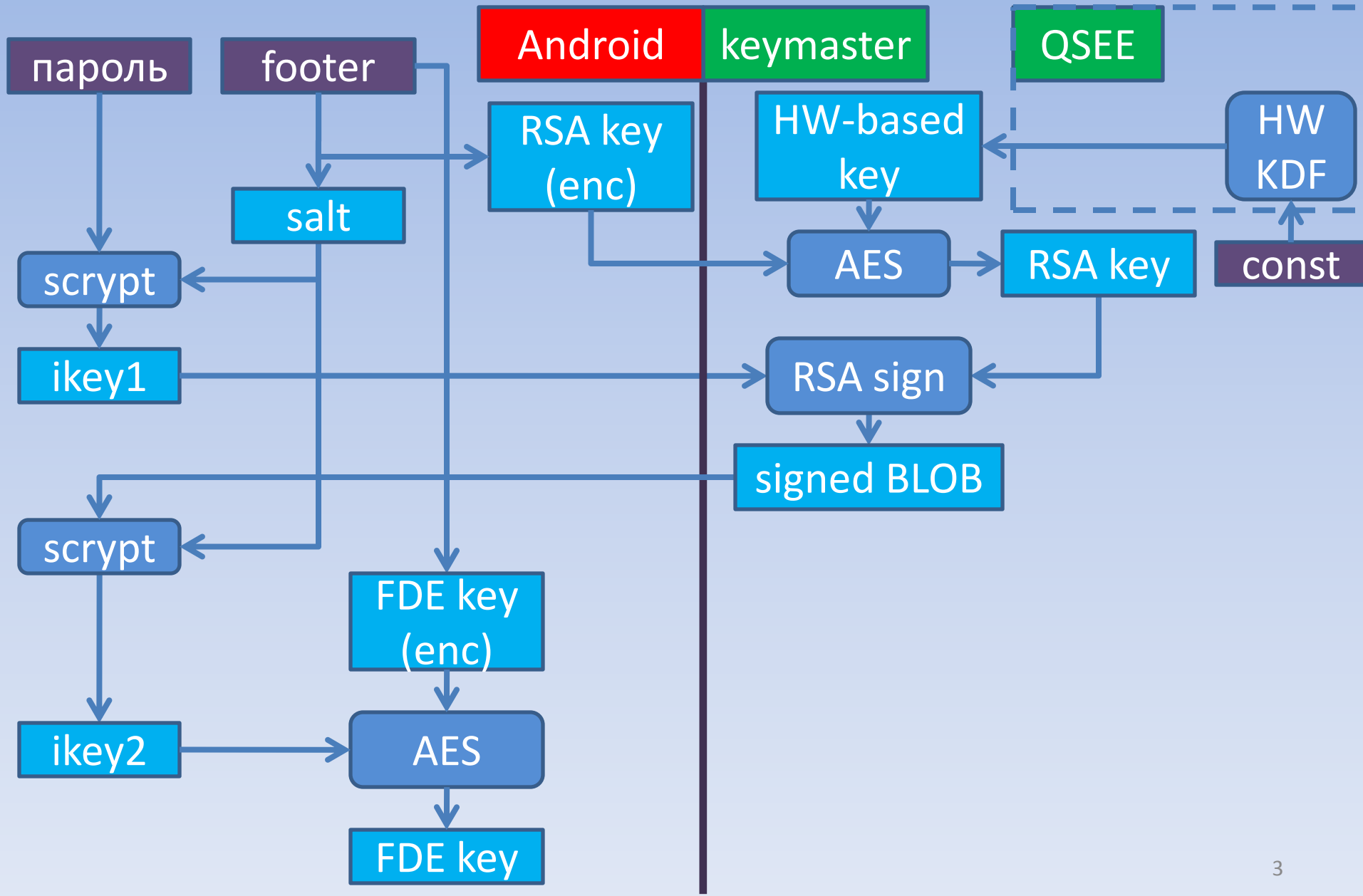
Хоруженко Г.И., Passware Inc.

21 марта 2018 г.

Актуальность

Версия ОС Android	**Функция вычисления ключа из пароля (KDF)**	**Решение для перебора без участия телефона (offline)**
4.3 (JellyBean) и ниже	PBKDF2	+
4.4 (KitKat)	scrypt	+
5 (Lollipop) и выше	**scrypt + keymaster**	**?**

Описание KDF (Android 5, Qualcomm)



Известные результаты

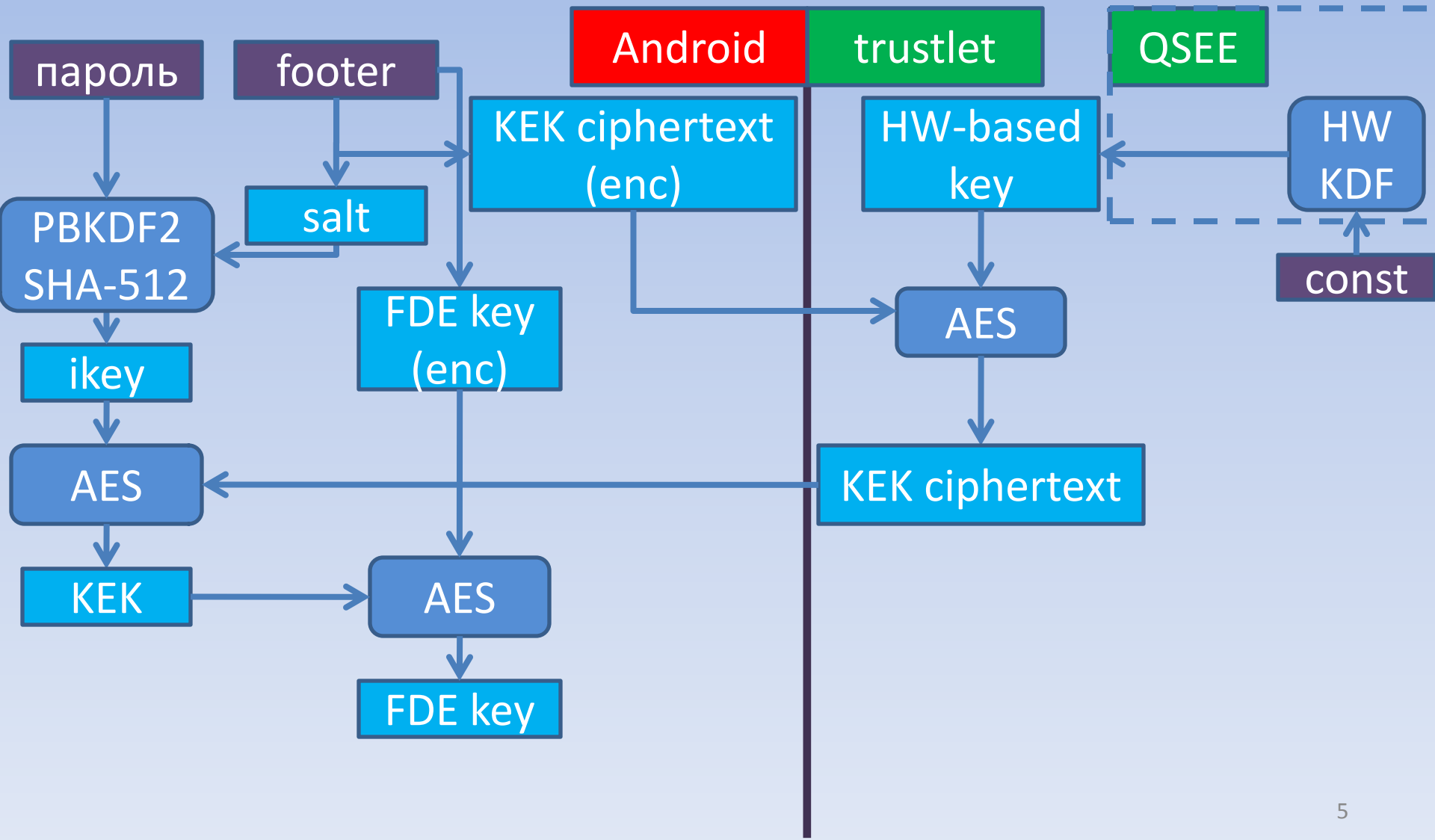
[1] L. Tóth, F. Spala "What's common in Oracle and Samsung? They tried to think differently...", 2013

Samsung S4 – offline-перебор

[2] F. Basse "Breaking Samsung Galaxy Secure Boot through Download mode", 2017

Samsung S5 – уязвимость в aboot (компрометация secure boot)

Описание KDF (Samsung G900P, Android 5-6, Qualcomm)



Ограничения имеющегося решения

Известное решение основывается на загрузке т.н. «**custom recovery**» на телефон с целью выполнения на нем произвольного кода.

- Заблокированный загрузчик - ?
- **Reactivation Lock/FRP -** ?

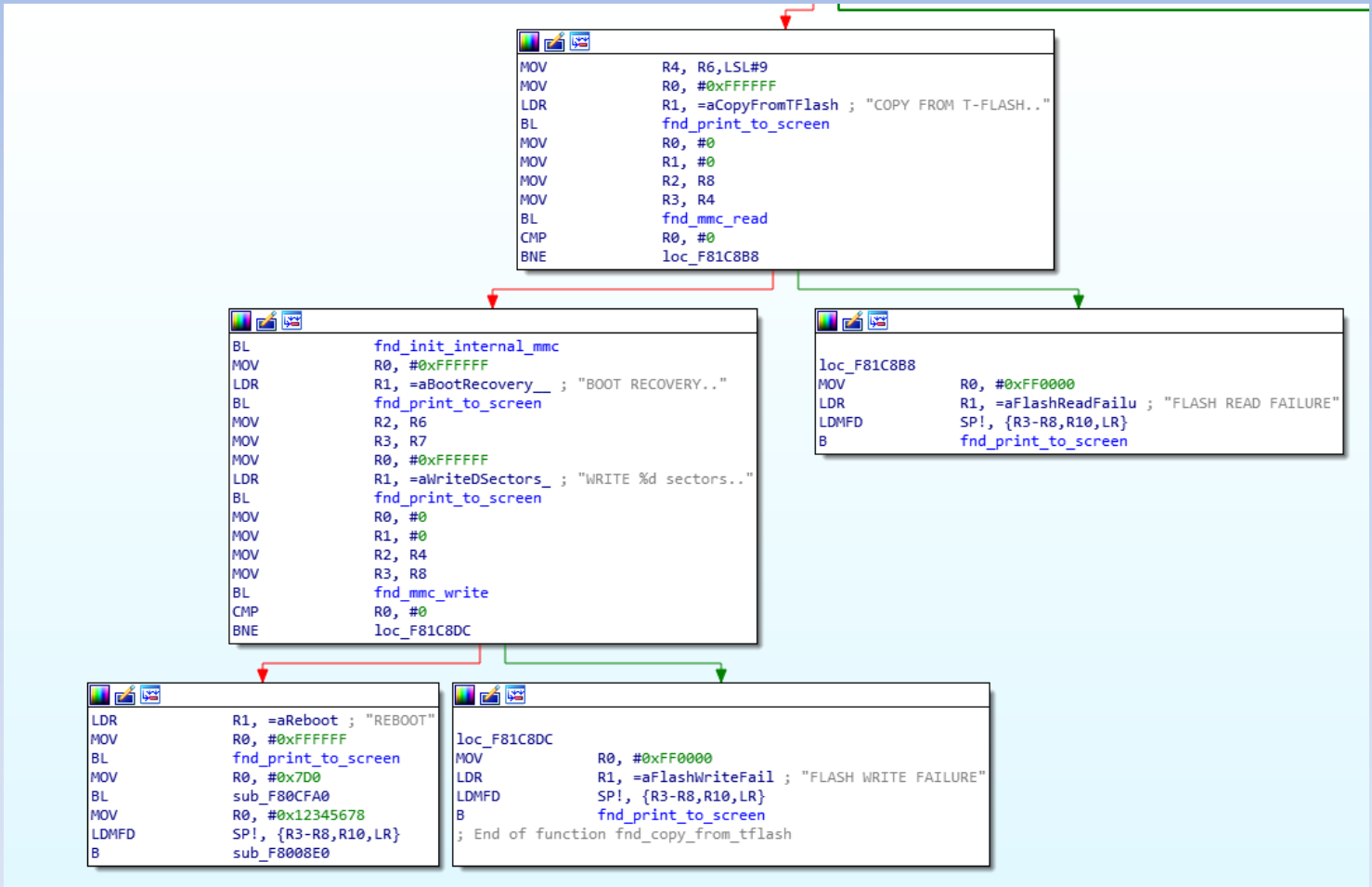
Предлагаемое решение

1. Получить управление в **aboot** (**write-what-where** примитив)
2. Загрузить **custom recovery** на **eMMC**
3. Отключить проверку подписи
4. Запустить **custom recovery**

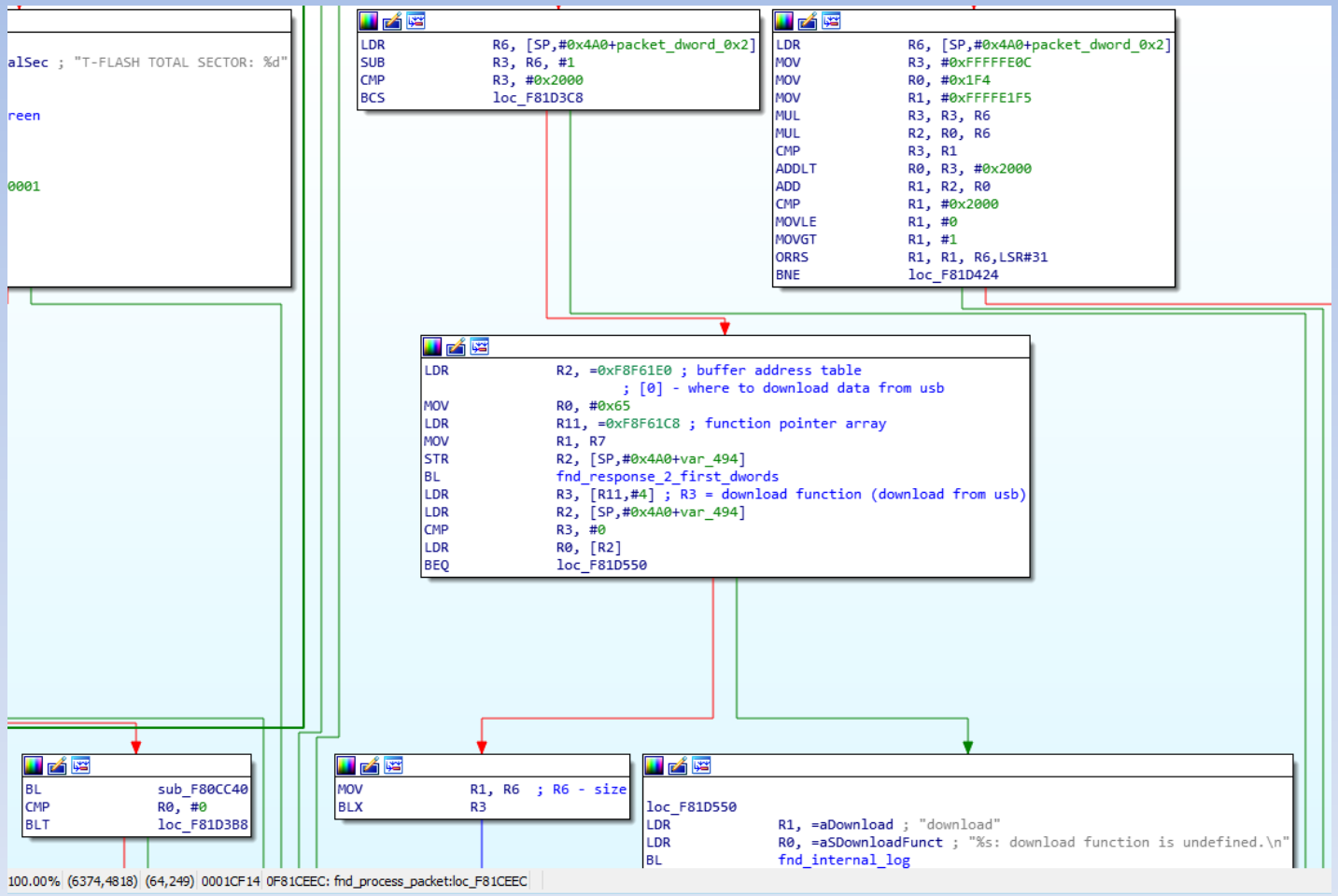
Вместо собственной реализации ключевых функций использовать имеющиеся в **aboot**:

- Вывод сообщений на экран (отладка)
- Прием/передача данных по **USB**
- Чтение/запись **eMMC**
- Управление загрузкой (загрузка **boot/recovery**)
- Проверка подписи

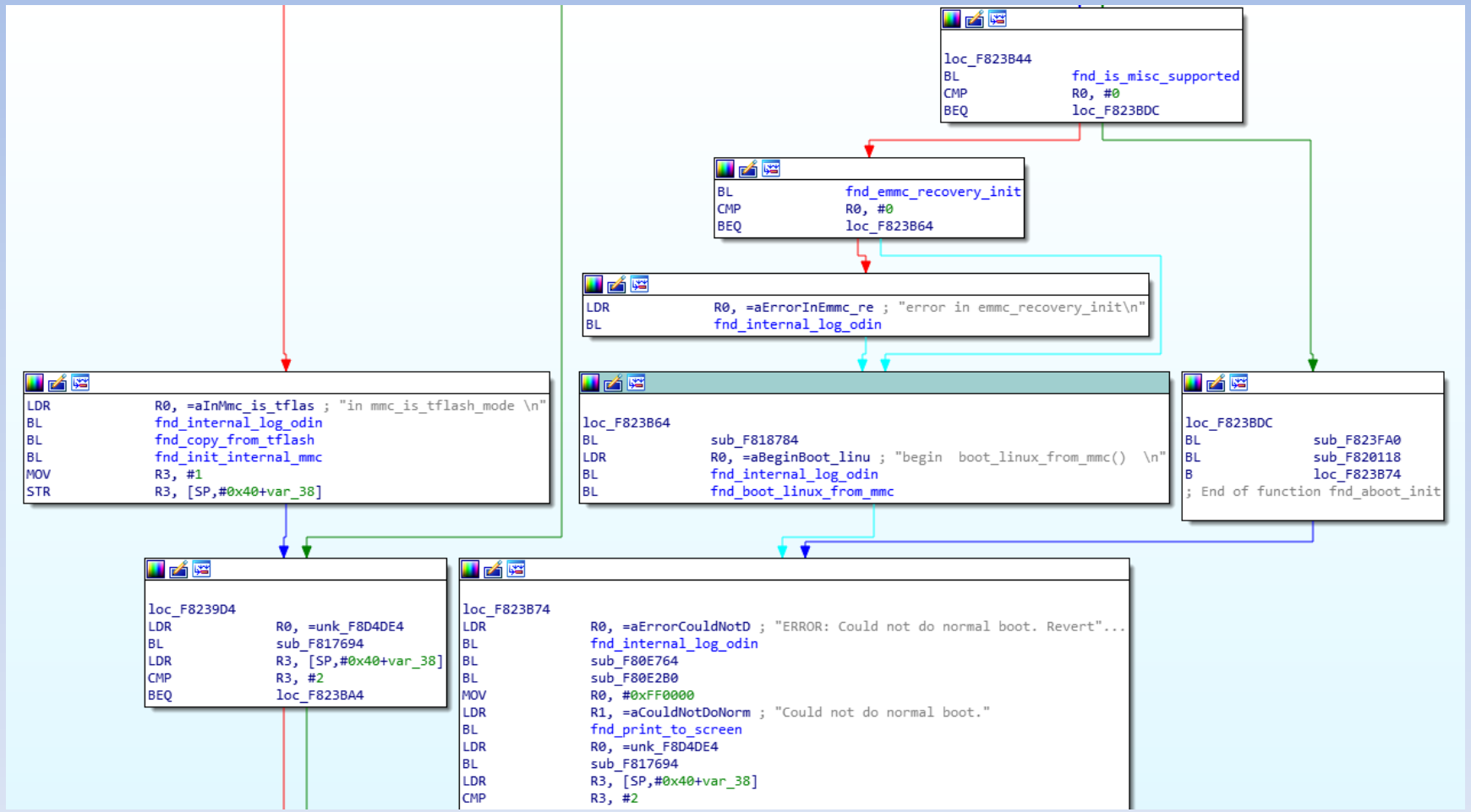
Поиск функций в aboot (1)



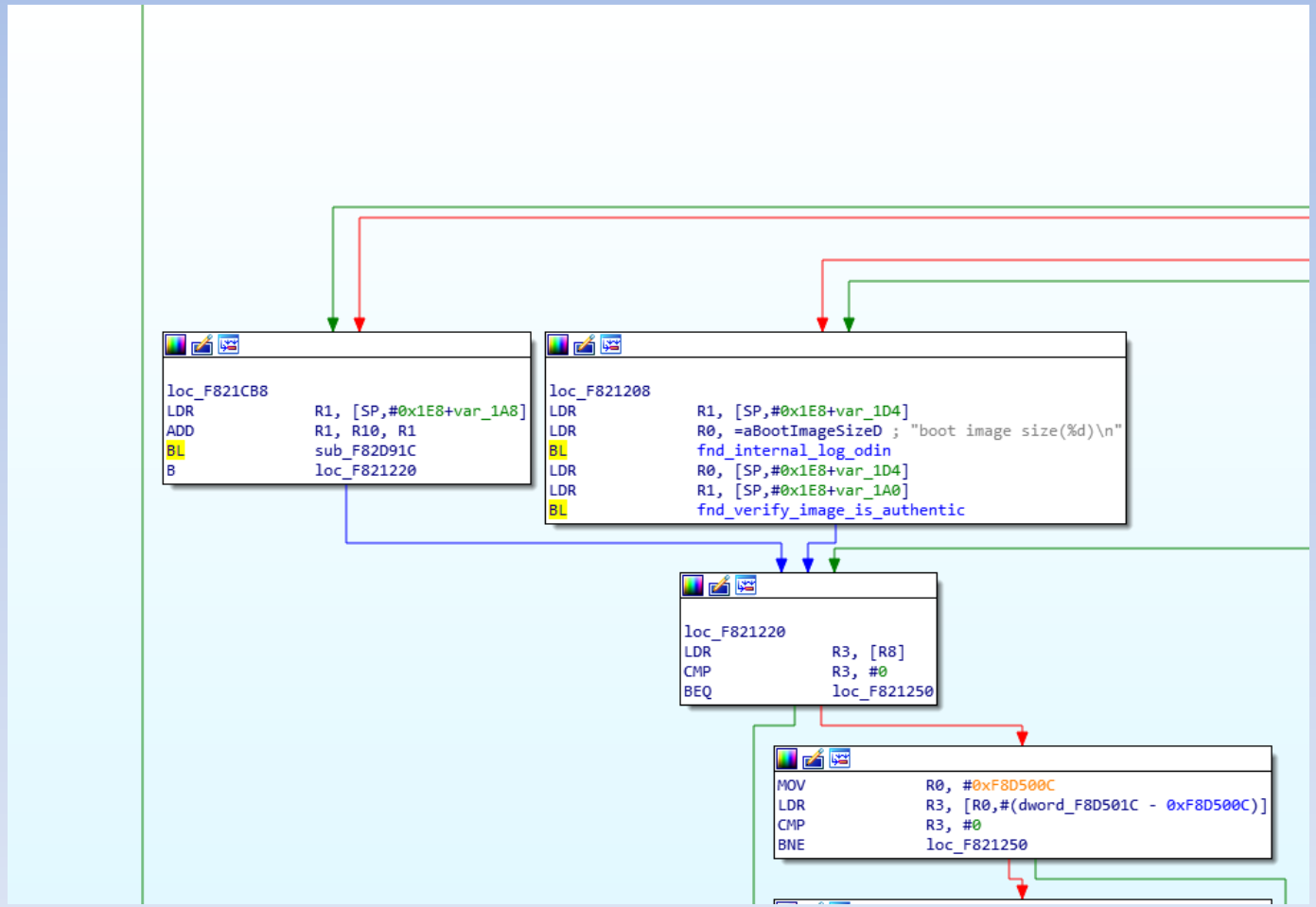
Поиск функций в aboot (2)



Поиск функций в aboot (3)



Поиск функций в aboot (4)



DEMO

Особенности решения

- Эксплойт написан для версии **G900PVPU3CPCA**

  “The issue has been reported to Samsung Mobile Security team on 2016-12-20 and is identifed as SVE-2016-7930. Patch was released in Samsung Security Bulletin of March 2017” [2]
- Актуальная версия – **G900PVPS3CQD1 (25.05.2017)** – при включенном **Reactivation Lock** допускает установку уязвимой версии **aboot** без удаления данных **userdata**
- **KNOX Warranty Void bit** не устанавливается

Результаты работы

- Обнаружена слабость криптографической схемы вычисления ключа шифрования для **FDE** в телефоне **Samsung S5 (G900P),** приводящая к возможности **offline**-перебора пароля
- Реализовано **программное** решение, позволяющее осуществлять **offline**-перебор пароля на **G900P** в обход **Reactivation Lock** (в том числе, на **последней версии firmware**).
- Аналогичное решение проверено для **G900T1 (S5)**, **I545 (S4)**

Спасибо за внимание!