Особенности извлечения данных из Android Go устройств

Карондеев Андрей, специалист отдела исследований мобильных устройств

Оксиджен софтвер

Android Go


android
Go edition
180+
countries
1600+
device models
$77
Tecno Spark 2
$73
Samsung A2
$62
Xiaomi Redmi Go
$64
Itel s15
$59
Nokia 1
$33
Safaricom Neon Storm
$27
Mobicel Astro

Android Go

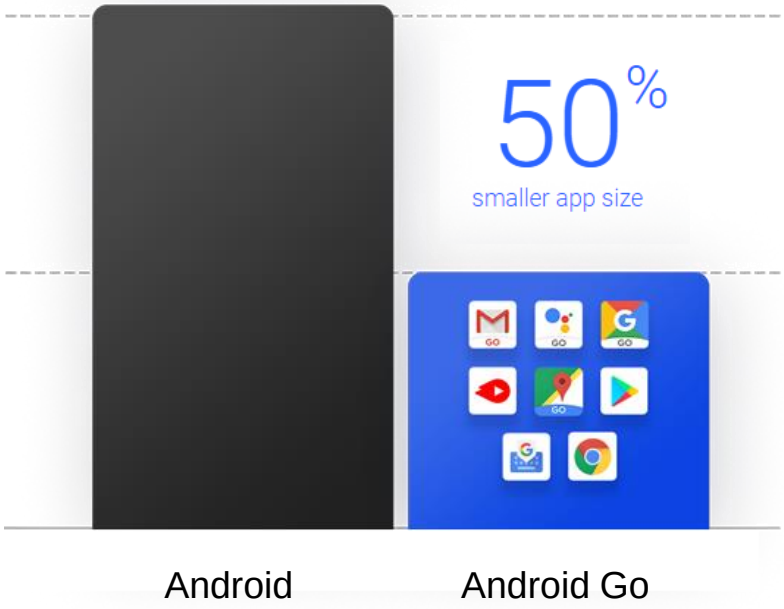
- Отключена функция бесшовного обновления системы

8Gb ROM Android

8Gb ROM Android Go

Android Go

- Уменьшен размер приложений
- Ограничен размер фоновых данных



Android Go

- Смартфоны начального уровня, которые имеют те же ключевые функции безопасности, что и Android

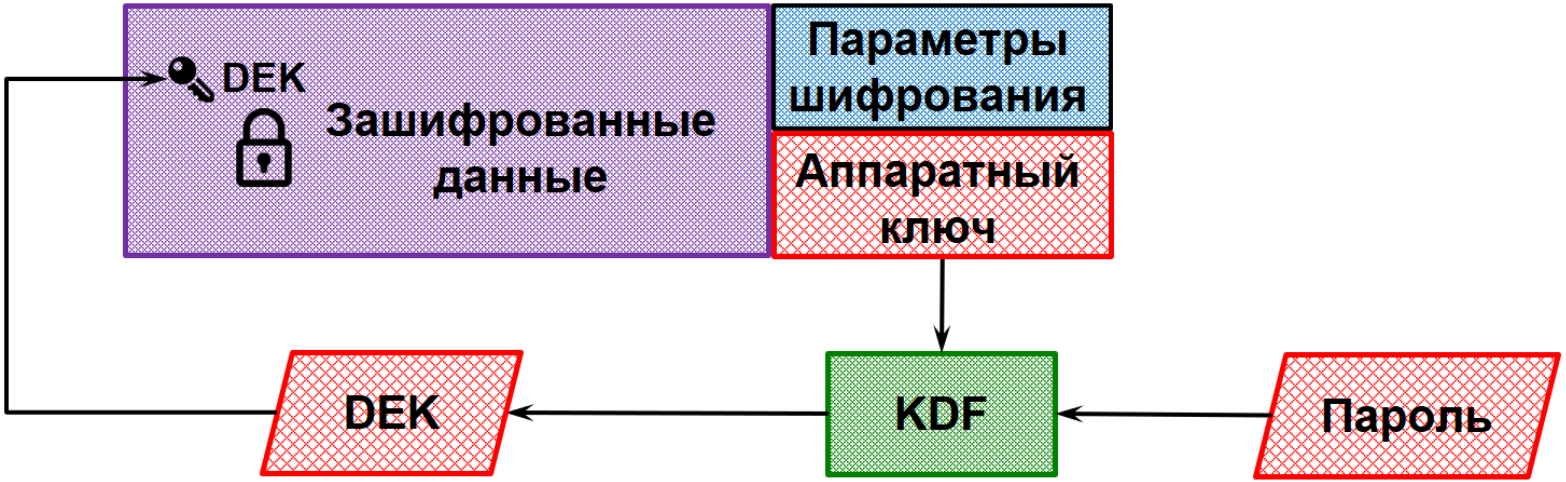
Проблема шифрования данных

Версия Android	Пользовательские данные зашифрованы по умолчанию	шифрование аппаратным ключом
Android 4	Нет	Не поддерживается
Android 5	Следует	Обязательно*
Android 6	Следует	Обязательно*
Android 7	Обязательно	Обязательно*
Android 8	Обязательно	Обязательно
Android 9	Обязательно	Обязательно
Android 10	Обязательно FBE	Обязательно

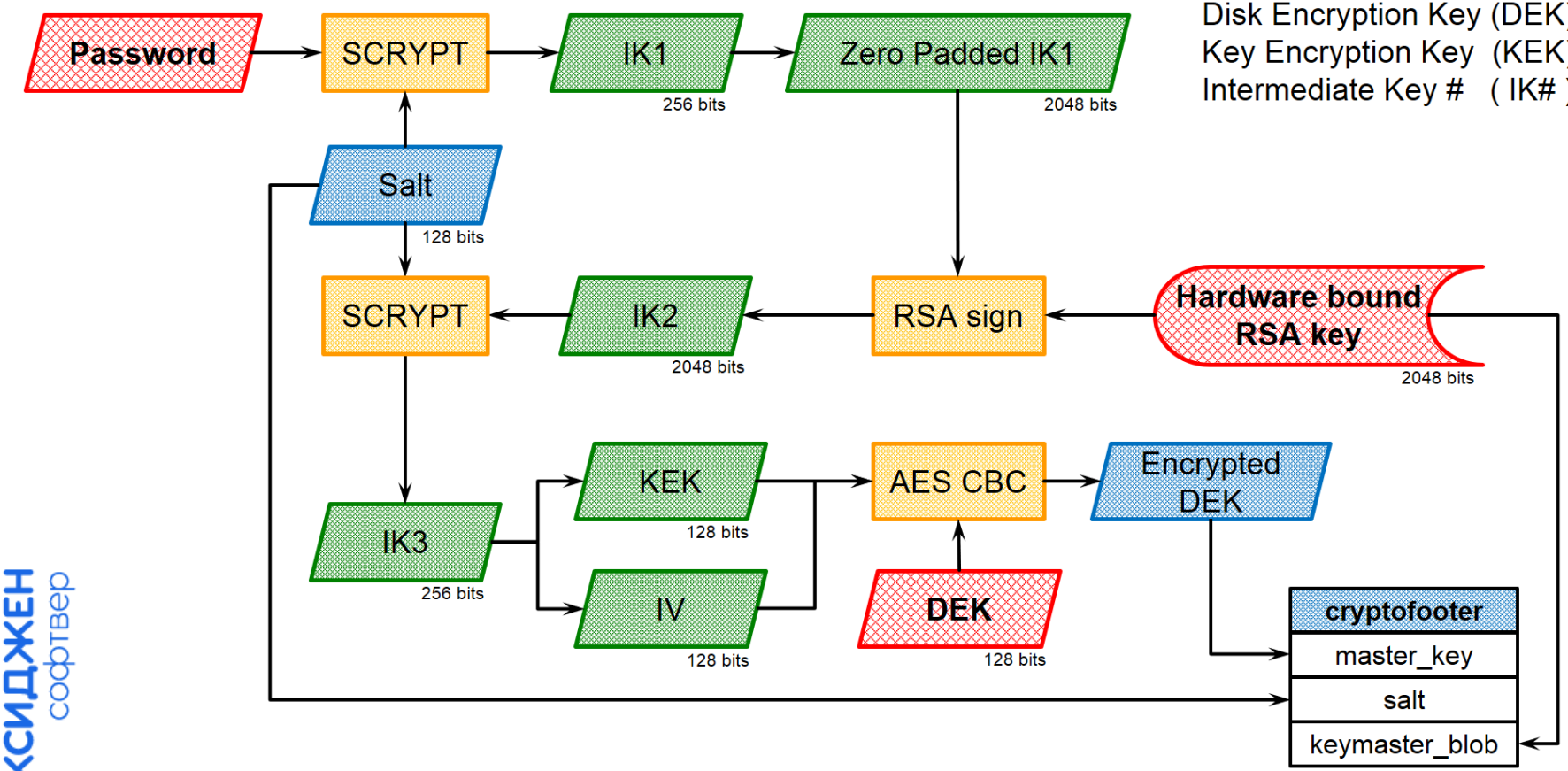
*) Если устройство поддерживает аппаратное хранилище ключей

https://source.android.com/compatibility/cdd

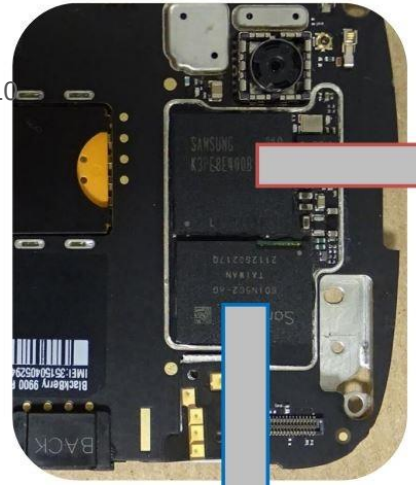
Шифрование пользовательских данных



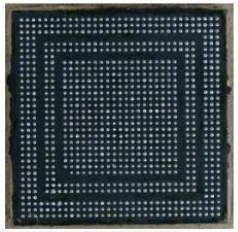
Ключ шифрования устройства (Device Encryption Key - DEK)
Функция выработки ключа (Key Derivation Function - KDF)



Address	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f	Dump
00000000	c4	b1	b5	d0	01	00	03	00	30	09	00	00	00	00	00	00	Д±µР....0.....
00000010	10	00	00	00	03	00	00	00	bf	5f	39	03	00	00	00	00	.....ї_9.....
00000020	01	00	00	00	61	65	73	2d	63	62	63	2d	65	73	73	69	....aes-cbc-essi
00000030	76	3a	73	68	61	32	35	36	00	00	00	00	00	00	00	00	v:sha256........
00000040	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....
00000050	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....
00000060	00	00	00	00	00	00	00	00	d8	91	6b	98	ef	4d	0b	e5	........Ш‘k.пМ.е
00000070	92	2f	c4	f1	b4	d8	50	8b	00	00	00	00	00	00	00	00	’/ДсґШР‹........
00000080	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....
00000090	00	00	00	00	00	00	00	00	69	3a	78	3c	f6	38	78	2a	........i:x<ц8x*
000000a0	e9	63	8d	11	af	c4	1b	54	00	8e	bf	72	06	00	00	00	йс..ЇД.Т.Ћїr....
000000b0	00	9e	bf	72	06	00	00	00	00	10	00	00	05	0f	03	01	.ћїr............
000000c0	bf	5f	39	03	00	00	00	00	00	00	00	00	00	00	00	00	ї_9.............
000000d0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....
000000e0	00	00	00	00	00	00	00	00	00	0c	00	00	00	58	a4	79	.............X¤y
000000f0	f5	87	92	f6	7a	75	30	6c	b8	a8	04	00	00	c4	66	ae	х‡’цzu0lёЁ...Дf®
00000100	0c	4e	87	80	65	75	05	bb	f1	a1	80	28	8a	85	ca	14	.N‡Ъeu.»сЎЪ(Љ…К.
00000110	b0	de	46	0e	1a	b9	c6	fe	c3	ba	fa	02	99	37	13	41	°ЮF..№ЖюГєъ.™7.A
00000120	ff	24	5d	b9	64	d2	79	bb	bd	e9	f2	41	57	e5	2a	eb	я$]№dTy»SйтAWе*л
00000130	97	4a	16	a8	dd	9b	12	e7	be	2e	ba	8e	17	da	7c	42	—J.ЁЭ›.зs.єЋ.Ъ|B



Процессор



Аппаратный ключ

KDF

Память

User data

AES

ключ от данных

DEK

AES

Эфемерный ключ выработанный из пароля

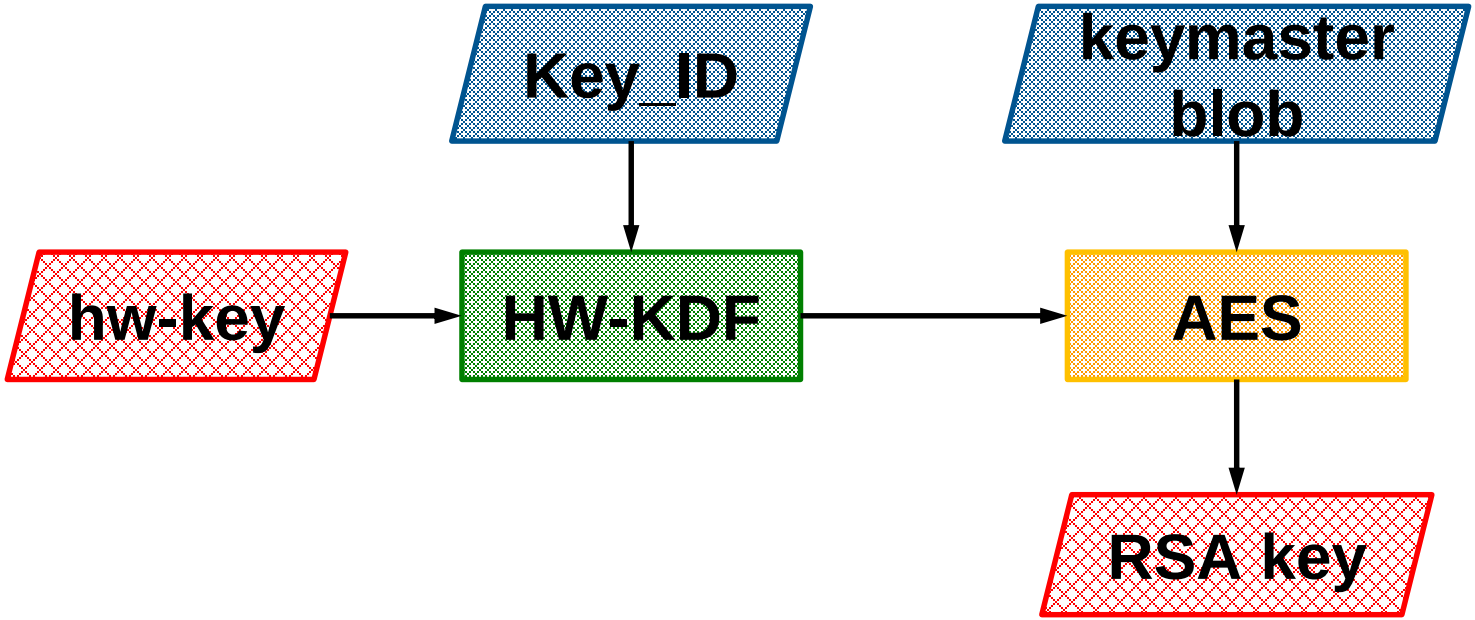
KEK

Оксиджен софтвер

Извлечение аппаратного ключа

- Позволяет подбирать пароль вне устройства
- Если подобран пароль, то позволяет расшифровать пользовательские данные

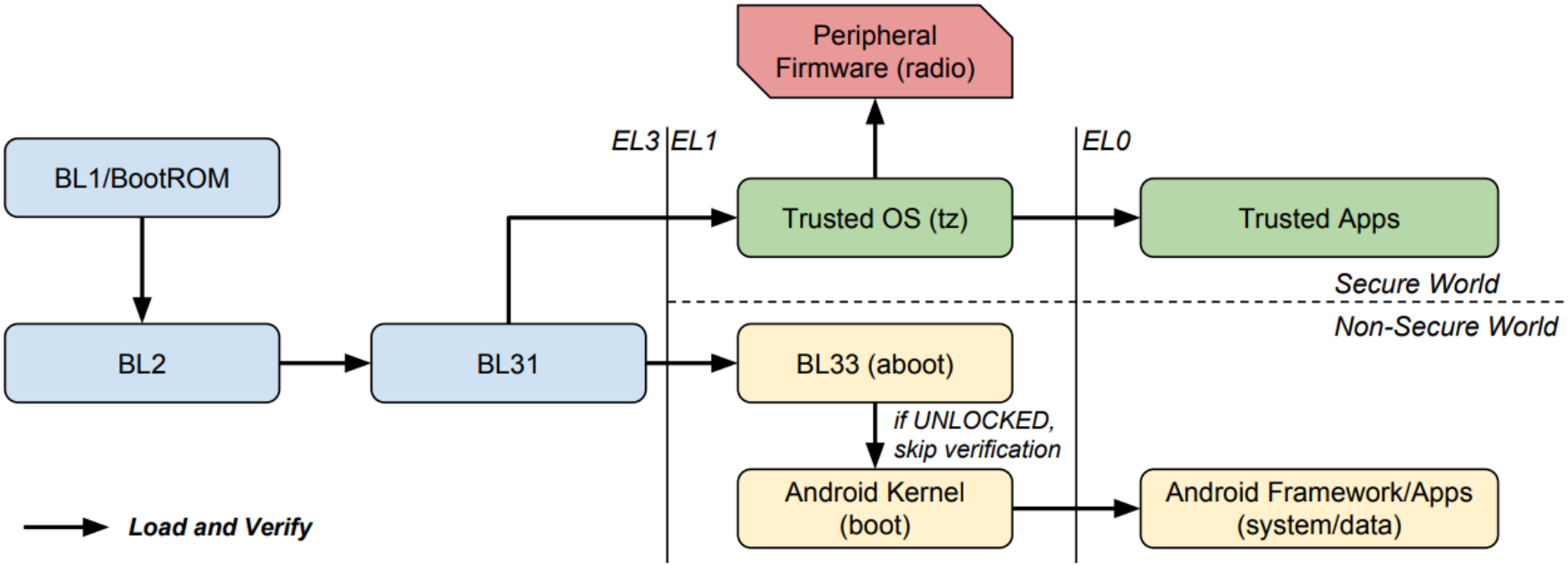
Извлечение аппаратного ключа



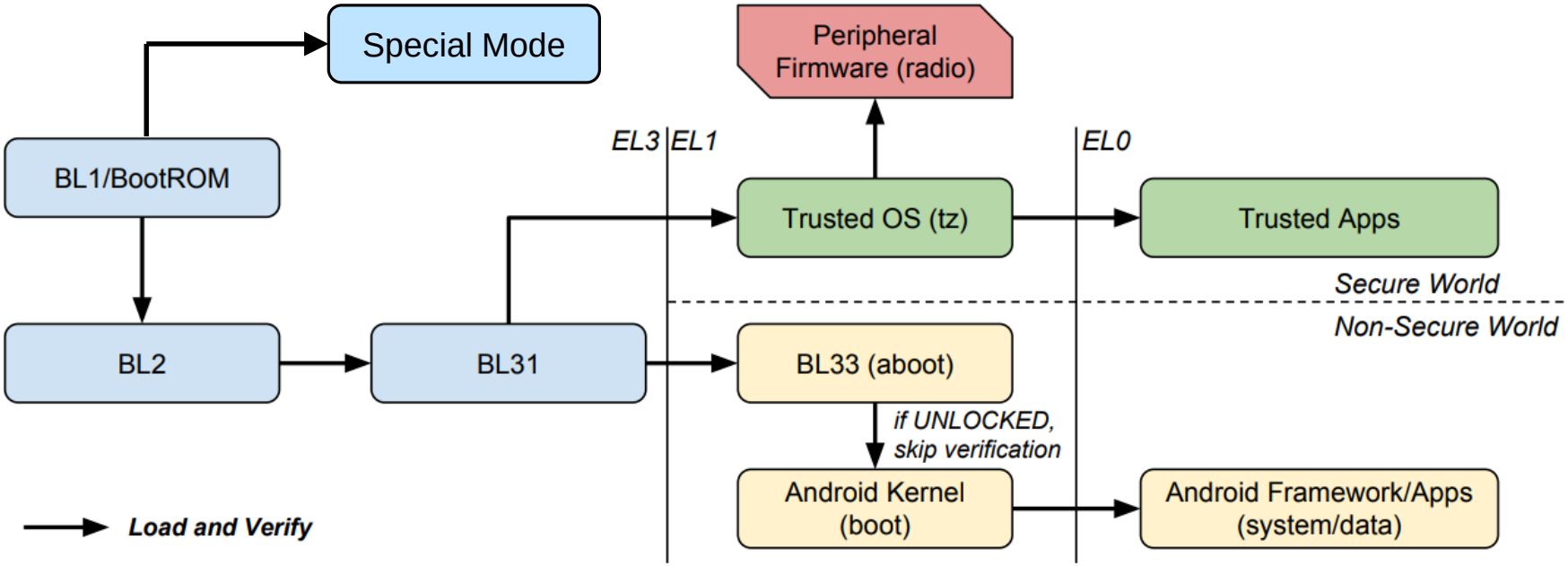
Извлечение защищенного на аппаратном уровне ключа

Принцип работы основан на эксплуатации уязвимостей в проприетарных протоколах, предназначенных для обновления ПО и диагностики Qualcomm, Exynos, MediaTek, Spreadtrum, Kirin устройств

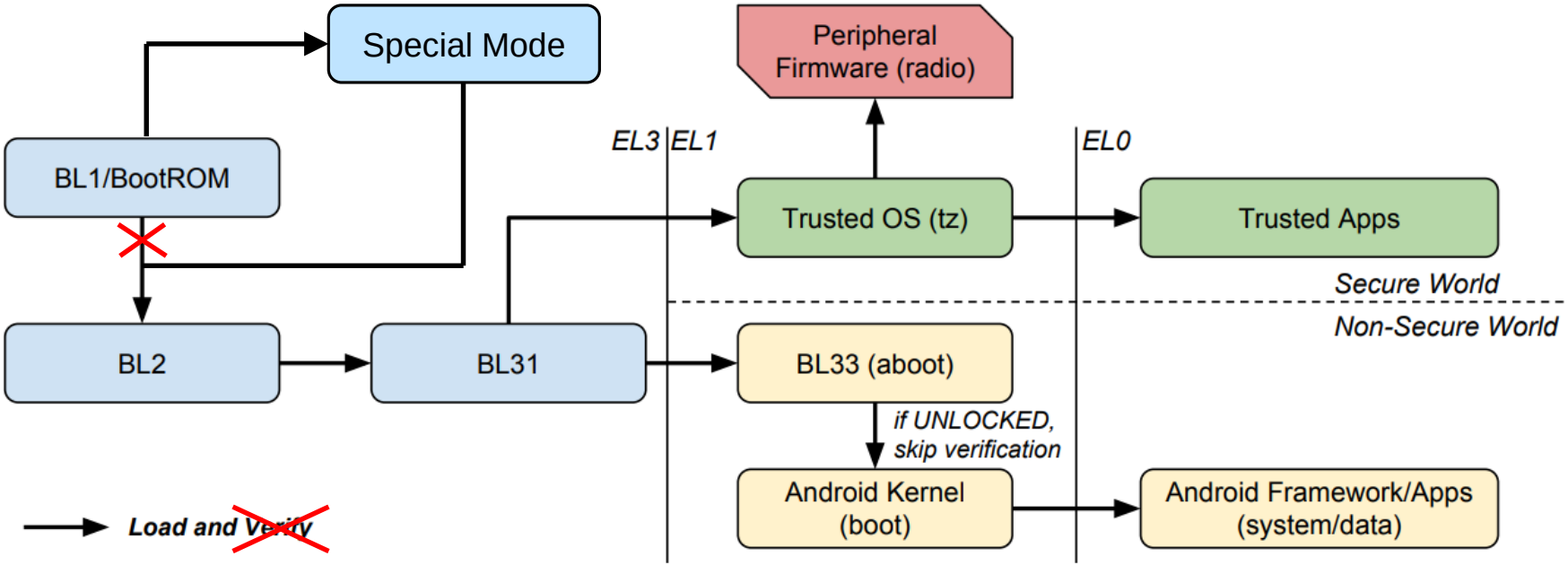
Извлечение защищенного на аппаратном уровне ключа



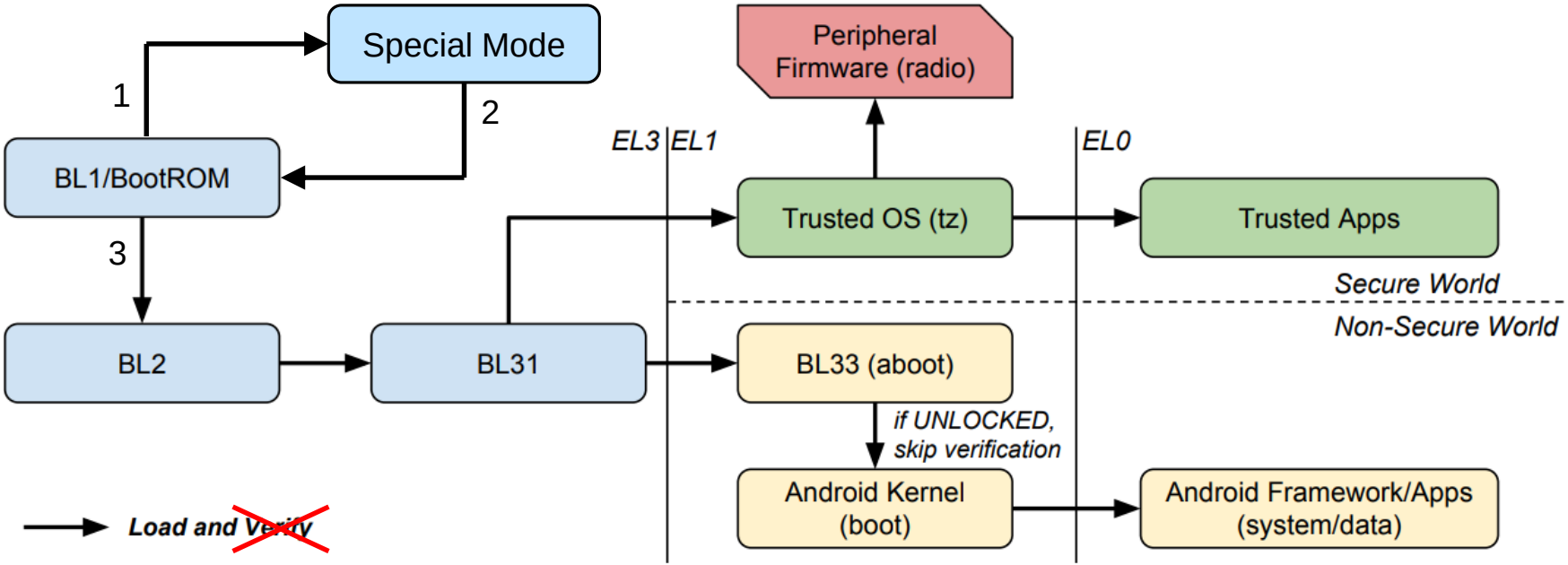
Извлечение защищенного на аппаратном уровне ключа



Извлечение защищенного на аппаратном уровне ключа



Извлечение защищенного на аппаратном уровне ключа



Android Go

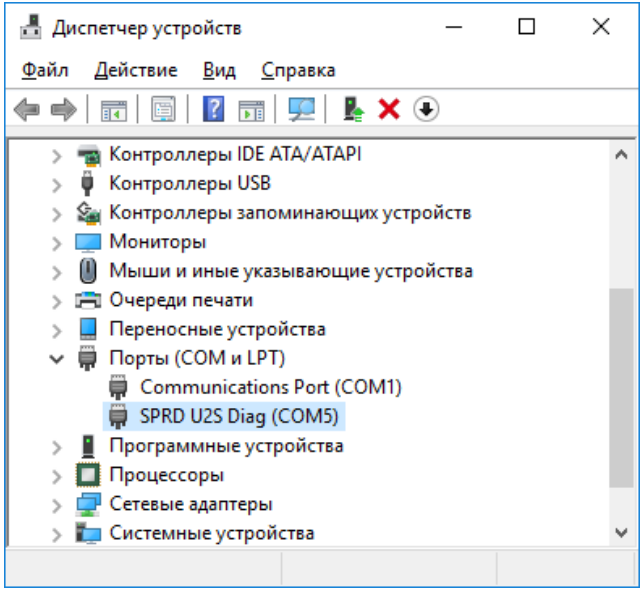
android Go edition

180+ countries | 1600+ device models

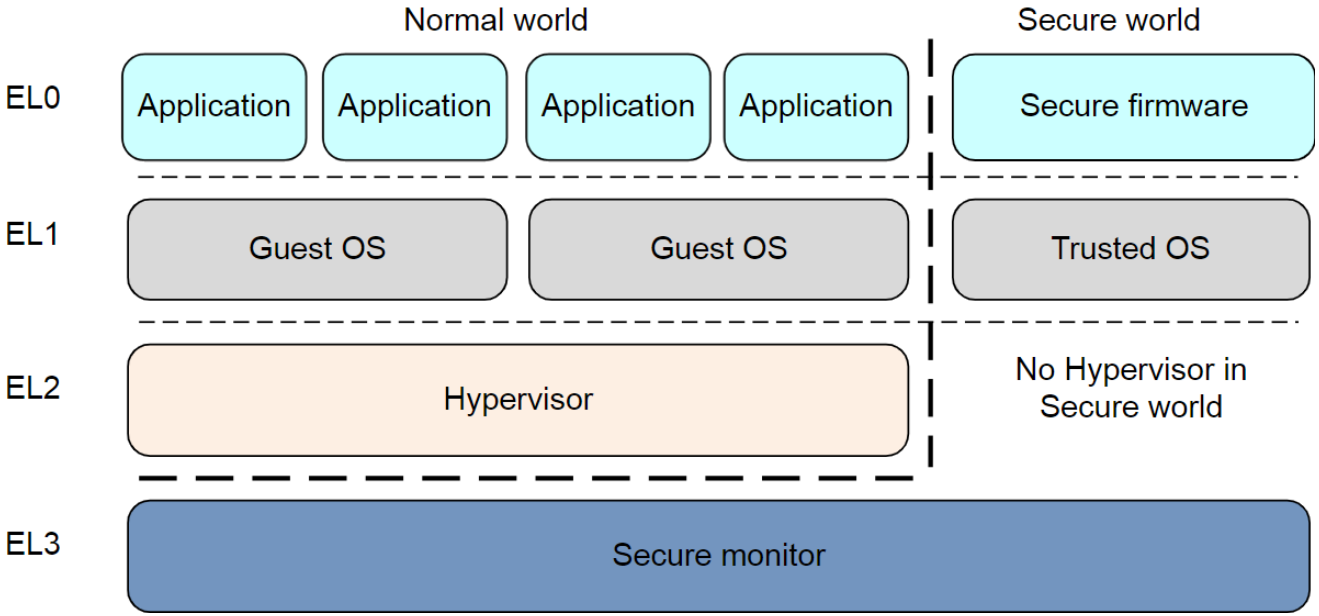
Tecno Spark 2	Samsung A2	Xiaomi Redmi Go	Itel s15	Nokia 1	Safaricom Neon Storm	Mobicel Astro
MT6580	7870	MSM8917	SC7731E	MT6737m	SC7731E	SC7731E
2015	2016	2016	2018	2016	2018	2018

Spreadtrum (Unisoc) Download Mode

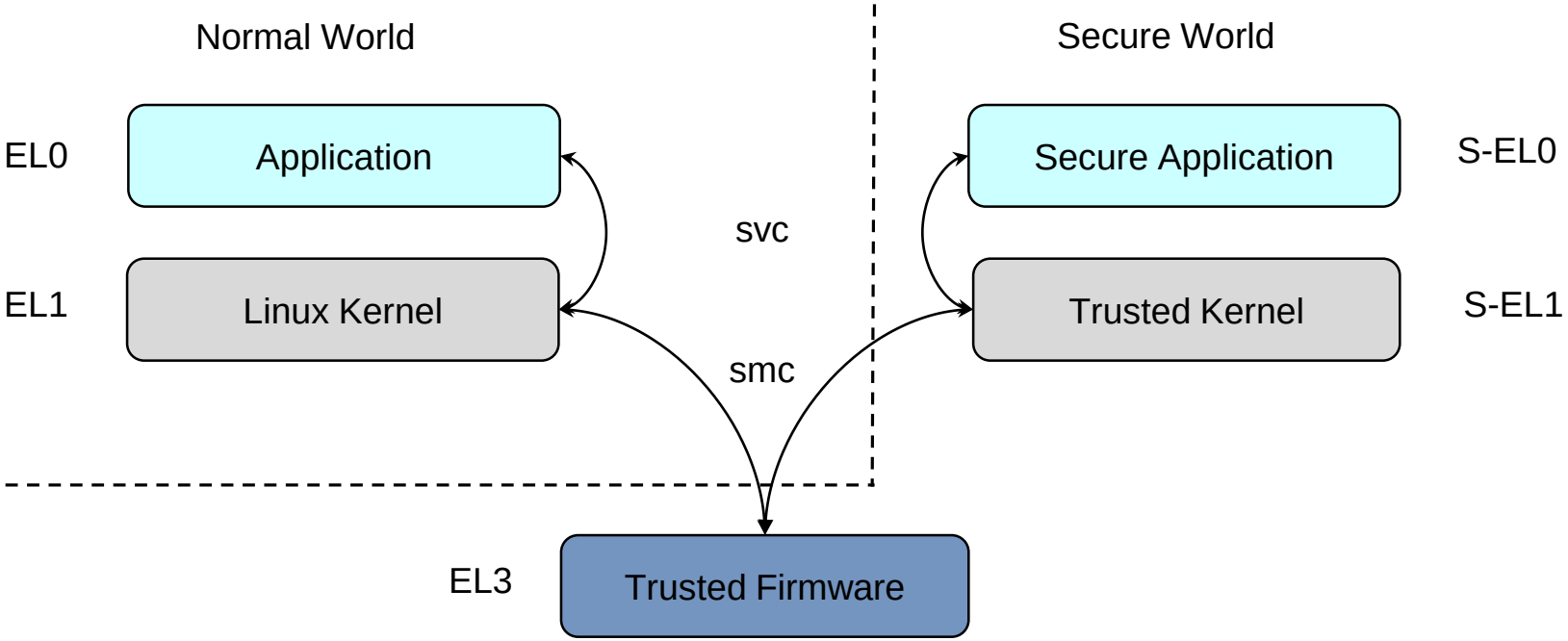
- На выключенном устройстве зажать кнопку volume down и подключить по USB
- Уязвимость в Download Mode позволяет получить возможность выполнить произвольный код в EL3
- Уязвимы SoC:
SC9850, SC7731E, SC9832E, SC9863



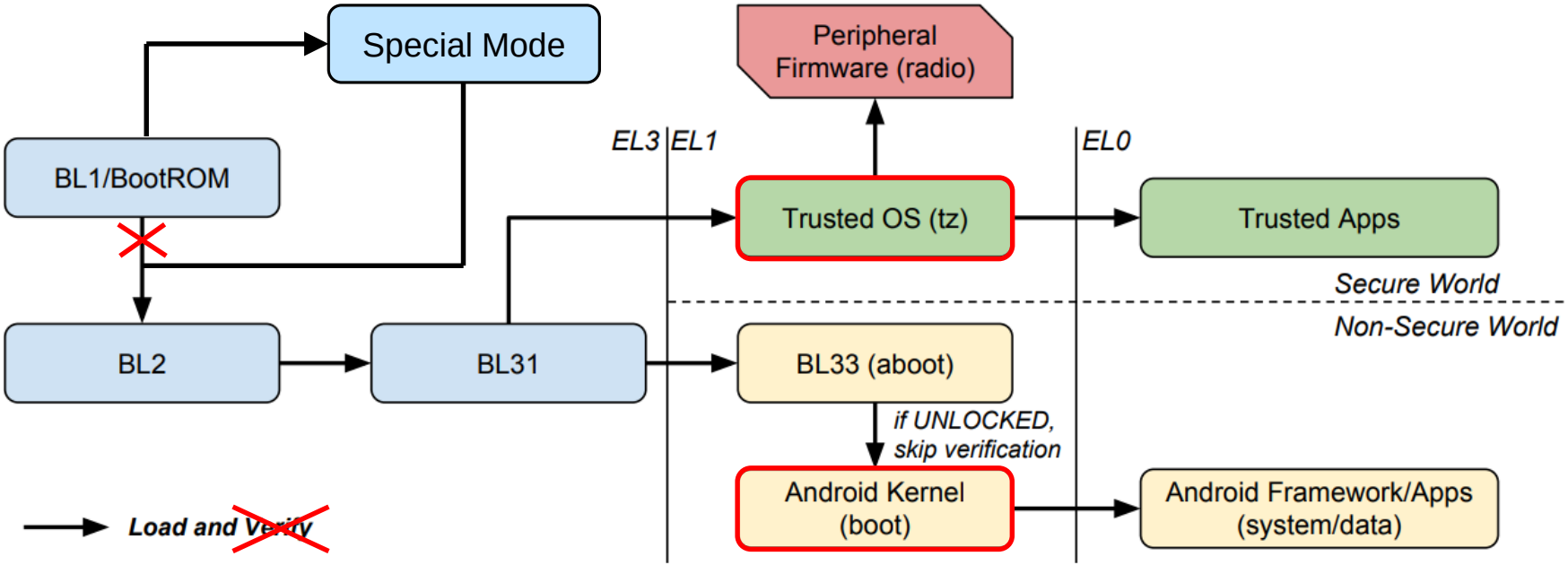
ARM TrustZone



ARM TrustZone



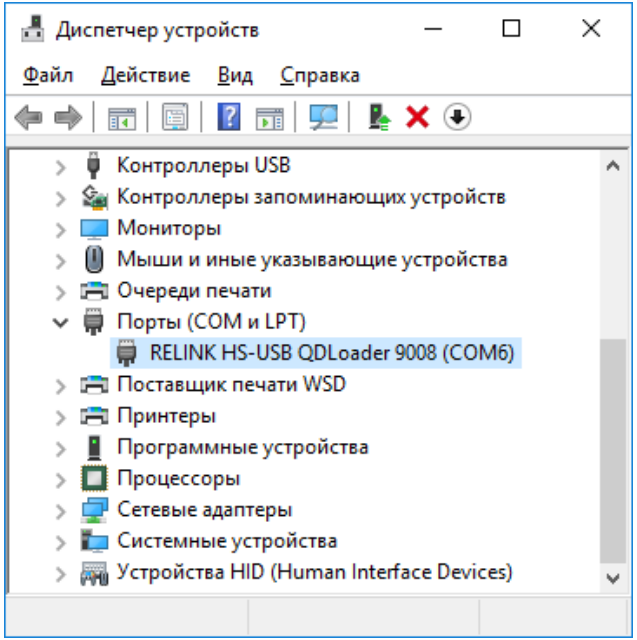
Извлечение защищенного на аппаратном уровне ключа



Qualcomm Emergency Download Mode* (EDL)

- Проприетарный протокол
- Низкоуровневые функции чтения/записи ROM
- Низкоуровневые функции чтения/записи RAM

*) Аварийный режим загрузки



Перевод в режим EDL

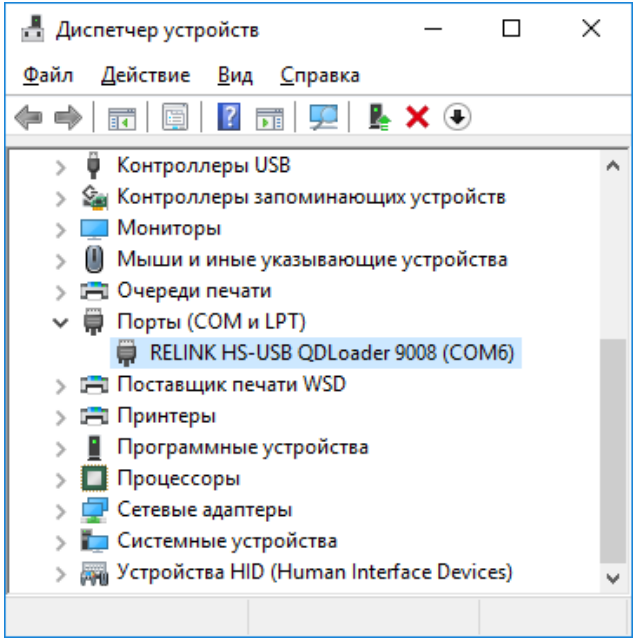
Замыкание контактов

- Test point
- eMMC CLK или DAT на GND


Xiaomi Redmi Go
Test Point
1+8G
4A904Z 24
IS 16046/IEC 62133
TIPS AND TRICKS
TRICKSBDINFO.BLOGSPOT.COM

Qualcomm Emergency Download Mode (EDL)

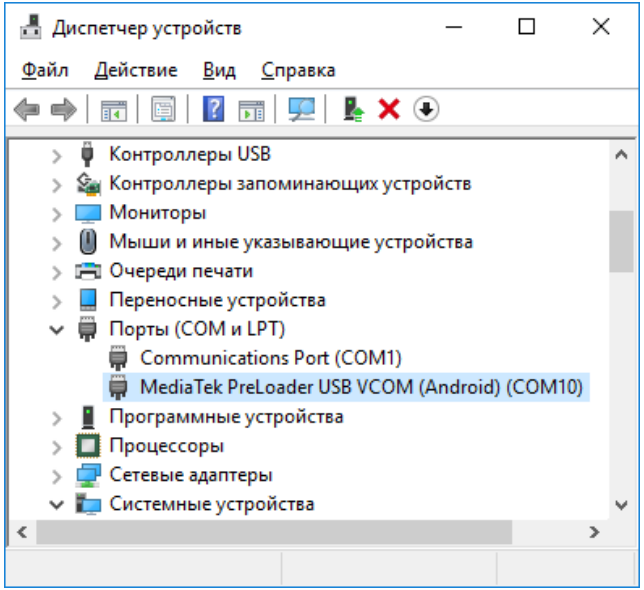
- Уязвимость в EDL позволяет получить возможность выполнить произвольный код в EL3



https://alephsecurity.com/2018/01/22/qualcomm-edl-1/

MediaTek DA режим

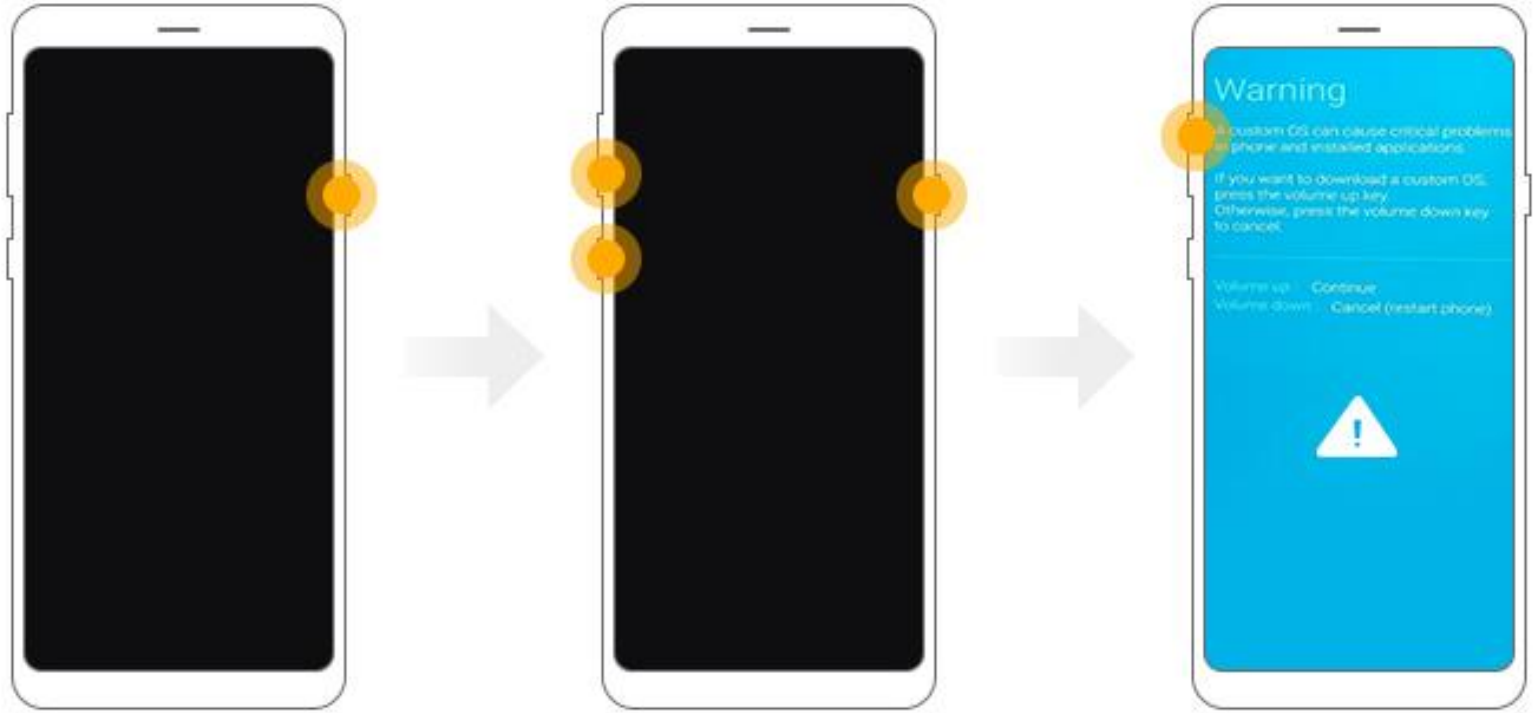
- Подключить выключенное устройство по USB
- Уязвимость в DA позволяет получить возможность выполнить произвольный код в EL3



MediaTek

- CVE-2020-0069
- Уязвимы все MediaTek arm64 устройства с обновлением безопасности до 01.03.2020

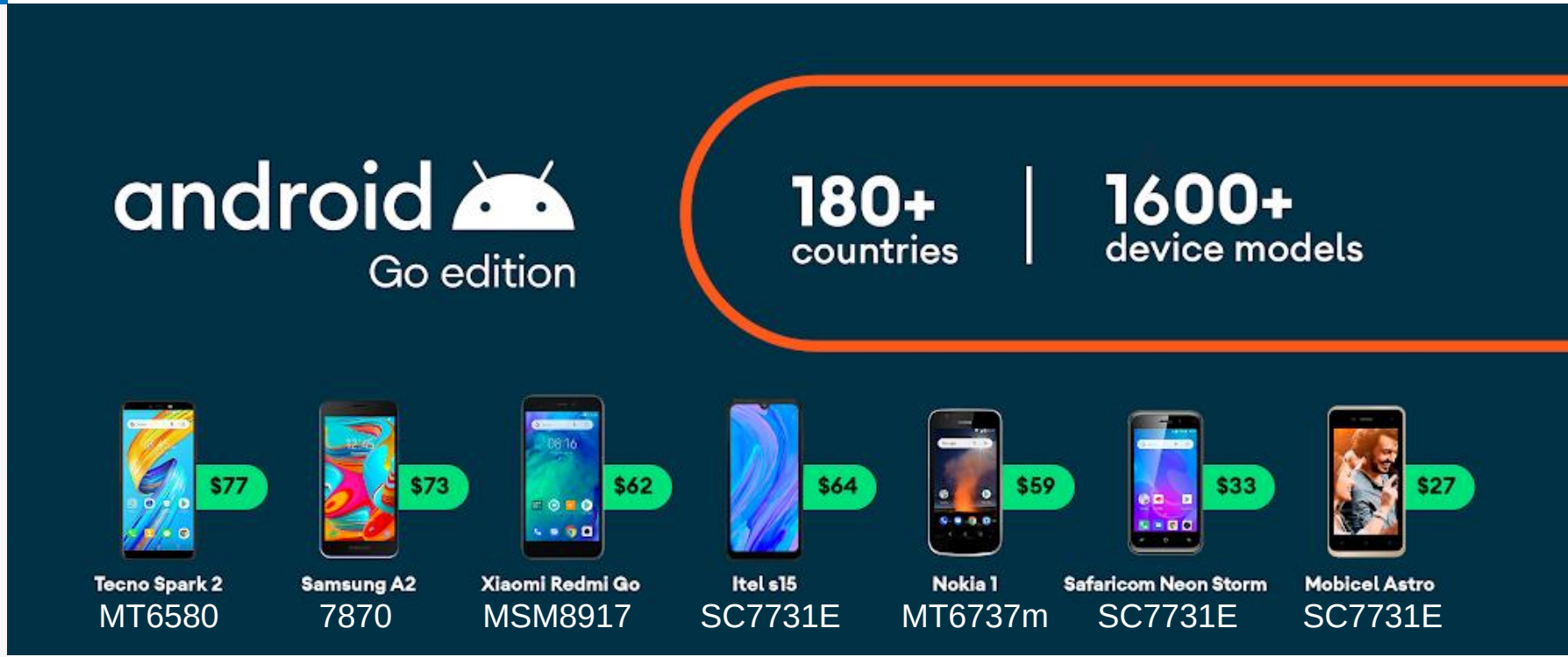
Samsung Odin



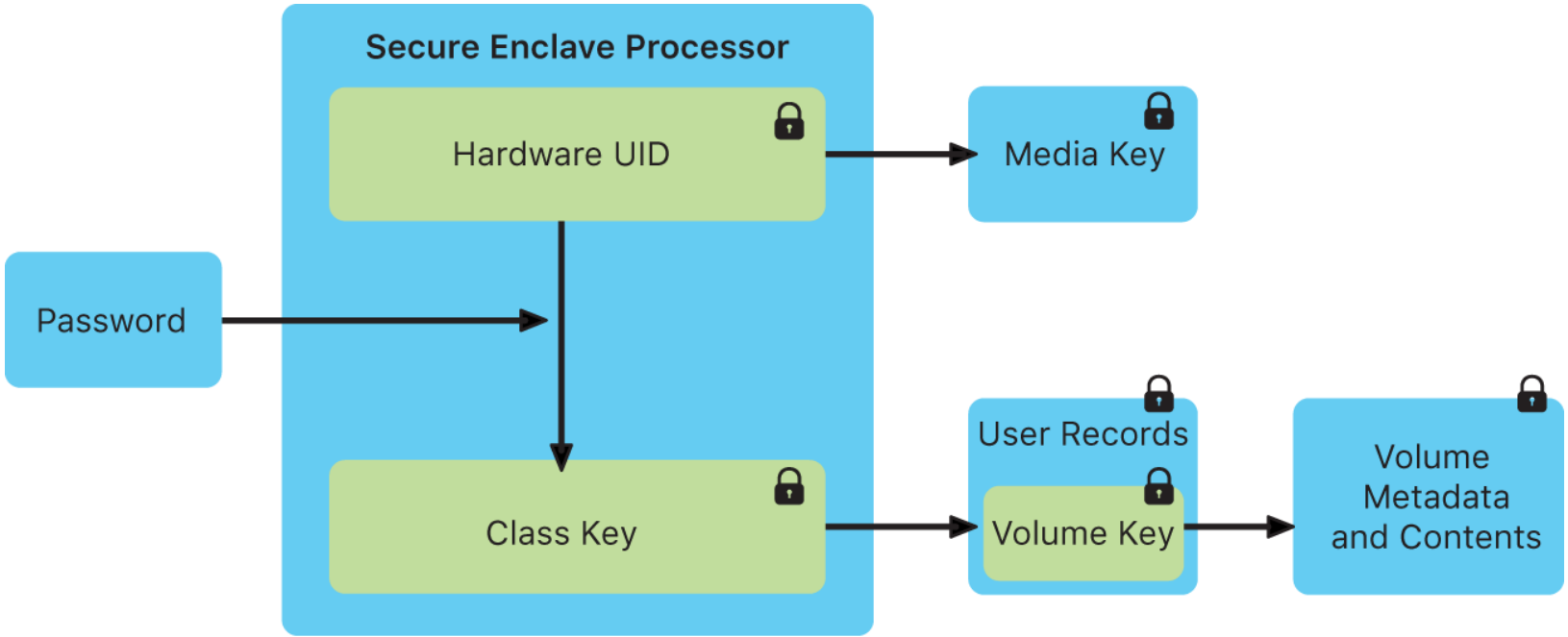
Уязвимости в Проприетарных протоколах

- MTK/Spreadtrum
- Qualcomm до MSM8996
- Samsung Exynos до 8910
- Apple iPhone X

Android Go



Apple Secure Enclave



Google Titan M

Titan™
Security

Подведем Итоги

- Для получения доступа к пользовательским данным необходимо знать или подобрать пароль
- В Android Go устройствах используются SoC, содержащие критические уязвимости
- Лучшее что можно сделать – извлечь защищенный на аппаратном уровне ключ и подбирать пароль вне устройства

Благодарю за внимание!

Оксиджен
софтвер