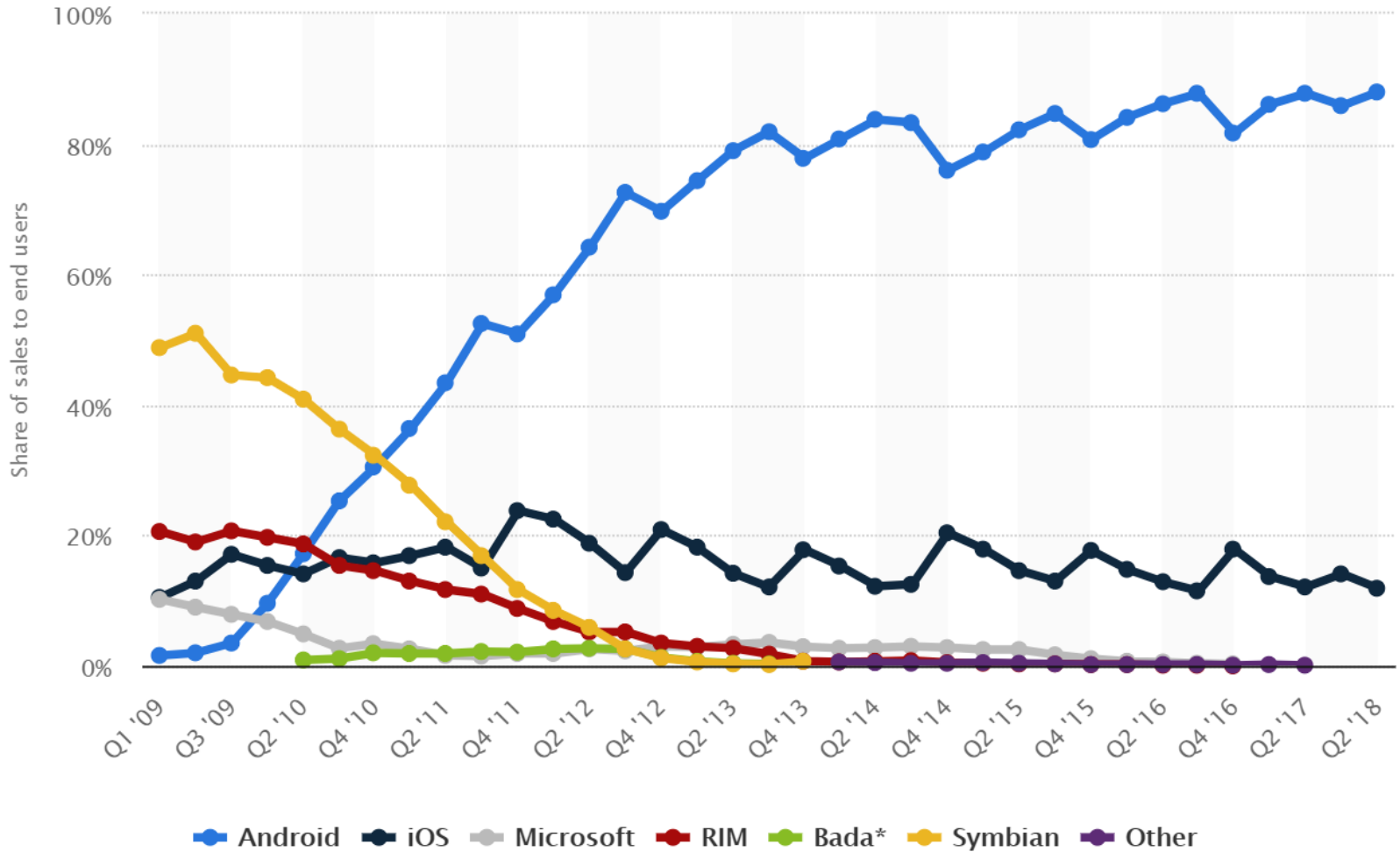
Мобильный Криминалист

Современные принципы шифрования Android-устройств и подходы к их расшифровыванию

Карондеев А.М.

2


100%
80%
60%
40%
20%
0%
Share of sales to end users
Q1 '09
Q3 '09
Q2 '10
Q4 '10
Q2 '11
Q4 '11
Q2 '12
Q4 '12
Q2 '13
Q4 '13
Q2 '14
Q4 '14
Q2 '15
Q4 '15
Q2 '16
Q4 '16
Q2 '17
Q2 '18
Android
iOS
Microsoft
RIM
Bada*
Symbian
Other

Android Compatibility Definition Document

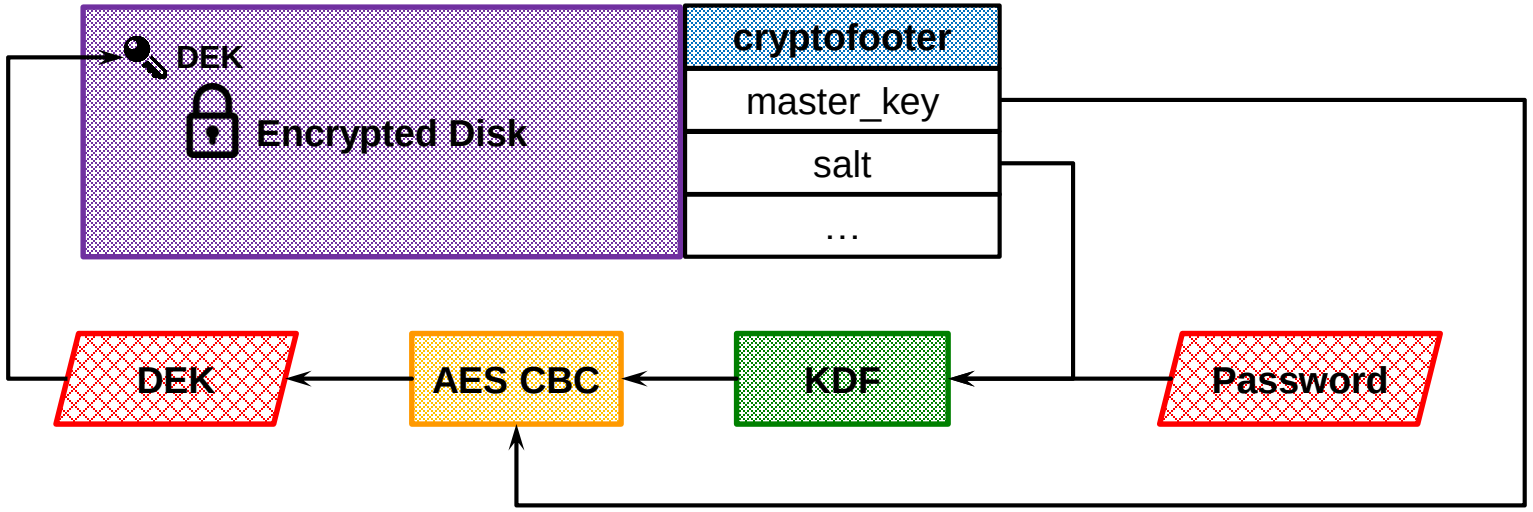
Android version	data storage encryption by default	hardware-backed keystore
Android 4	NOT	not supported
Android 5	SHOULD	MUST*
Android 6	SHOULD	MUST*
Android 7	MUST	MUST*
Android 8	MUST	MUST
Android 9	MUST	MUST

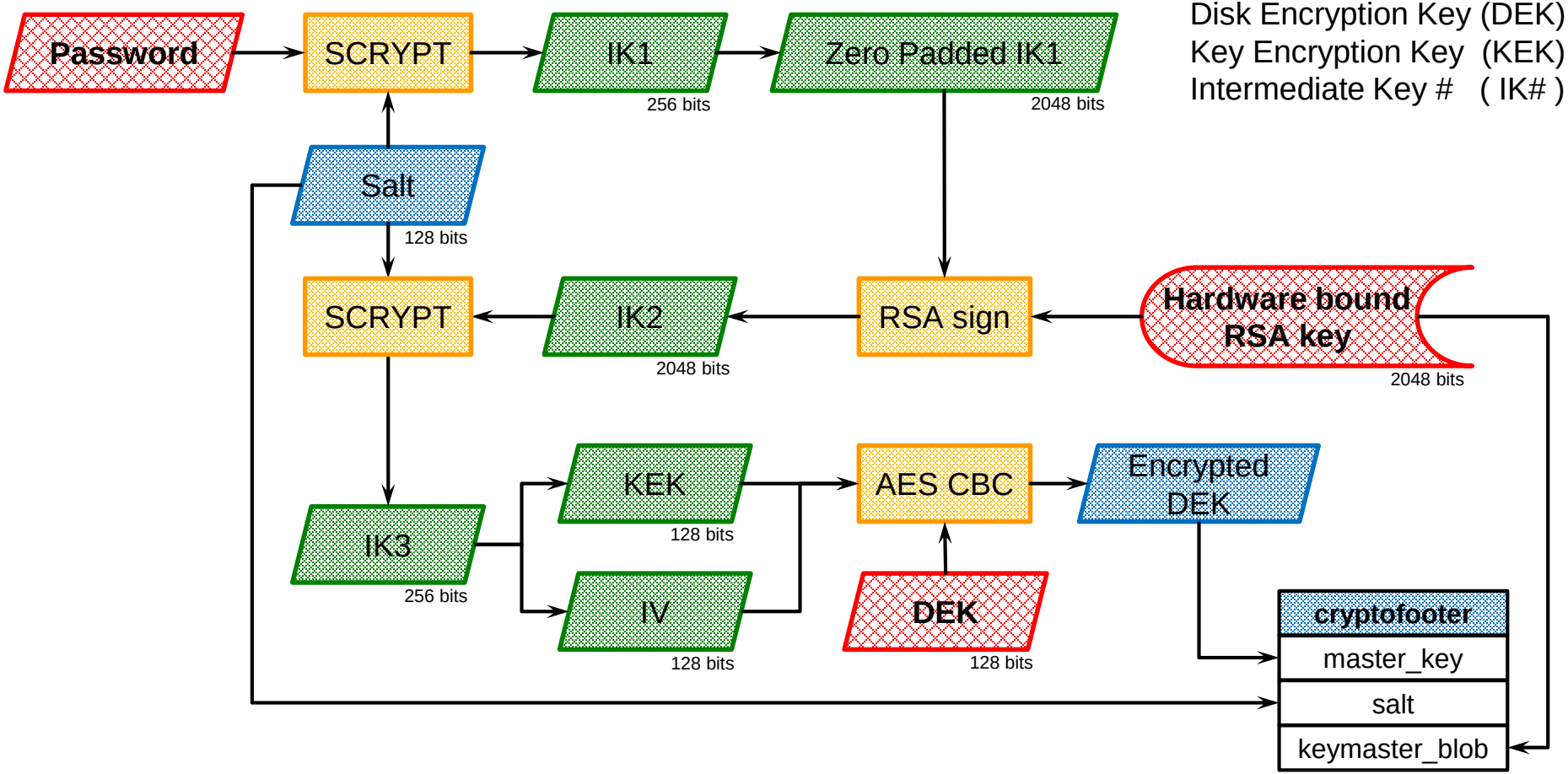
*) If the device provides a hardware-backed keystore

Мобильный Криминалист

http://www.мобильный-криминалист.рф

Android Full Disk Encryption





Подходы к расшифровыванию

- Уязвимости ОС
- Внедрение в процесс загрузки
- Извлечение hw-bound key

Мобильный Криминалист

http://www.мобильный-криминалист.рф

Уязвимости ОС

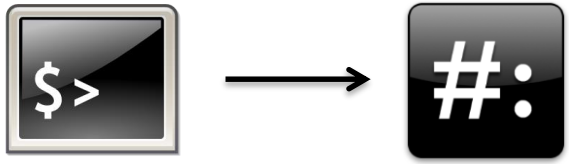
- Получение доступа Linux shell
- Повышение привилегий
- Чтение памяти

Мобильный Криминалист

http://www.мобильный-криминалист.рф

Уязвимости ОС

- CVE-2014-3153 (TowelRoot)
- CVE-2015-3636 (PingPong Root)
- CVE-2016-5195 (DirtyCow)
- CVE-2018-9445 (Smart adb)



Уязвимости ОС

Ограничения подхода:

- Необходимо разблокированное устройство
- После публикации уязвимости оперативно закрывают
- Среднее отставание порядка года

Мобильный Криминалист

http://www.мобильный-криминалист.рф

Внедрение в процесс загрузки

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

Мобильный Криминалист

http://www.мобильный-криминалист.рф

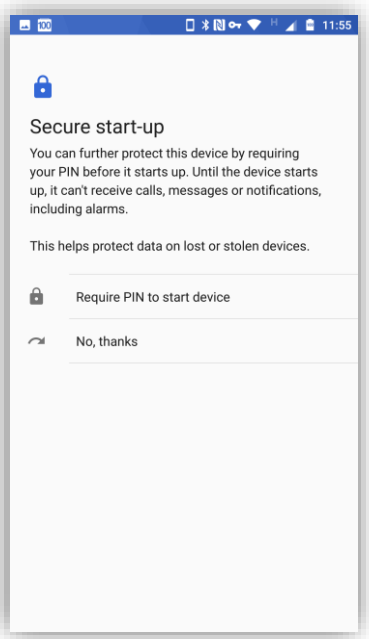
Внедрение в процесс загрузки

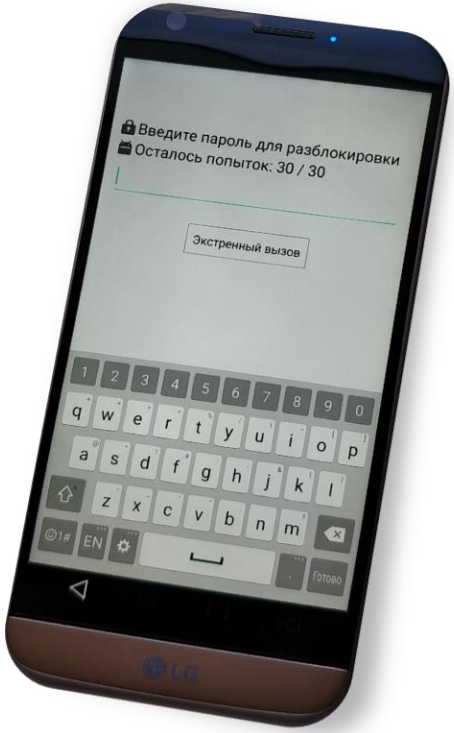
- Позволяет получить root shell до ввода
- Если известен пароль или выключена опция Secure Start-Up, то позволяет расшифровать userdata

Мобильный Криминалист

http://www.мобильный-криминалист.рф

Secure Start-Up

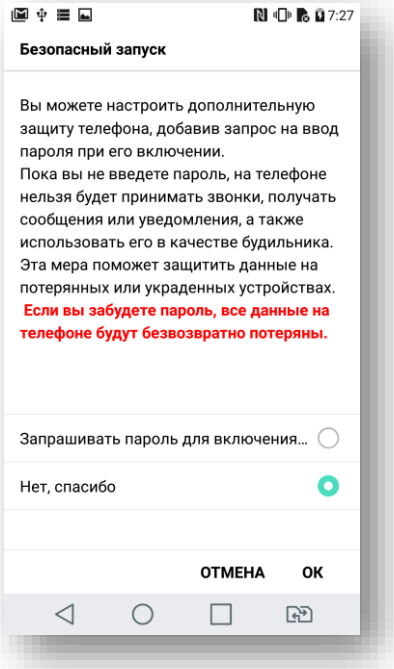


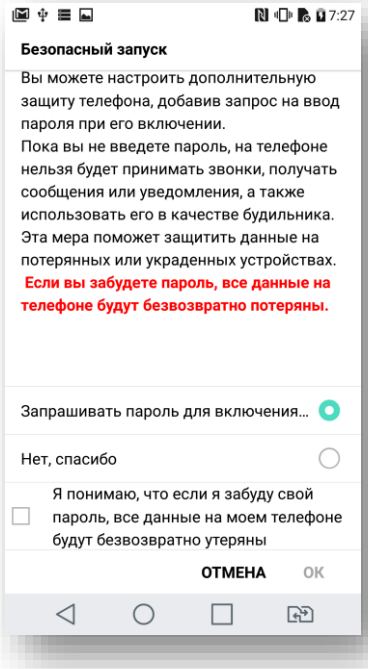


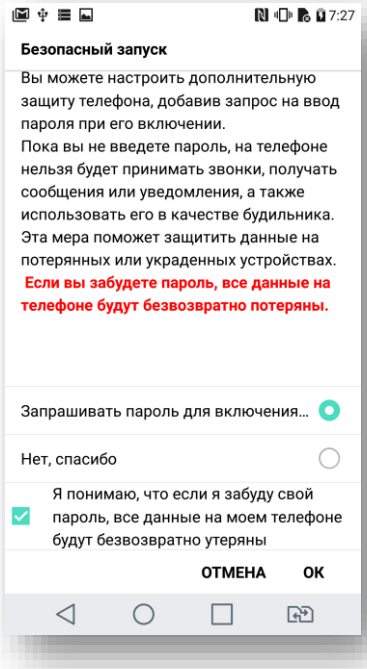
Мобильный Криминалист

http://www.мобильный-криминалист.рф

Secure Start-Up







Мобильный Криминалист

http://www.мобильный-криминалист.рф

Qualcomm Decrypting Bootloader

- Уязвимые SoC:
  msm8909, msm8916, msm8939, msm8952,
  msm8924, msm8994, msm8996, msm8976,
  msm8917, msm8937, msm8940, msm8953
- Уязвимые версии Android:
  до Android 7.1 включительно

Мобильный Криминалист

http://www.мобильный-криминалист.рф

Qualcomm Decrypting Bootloader

- Необходимо перевести устройство в режим EDL (9008)
- Необходим подписанный производителем firehose файл
- alephsecurity.com/2018/01/22/qualcomm-edl-1/

Мобильный Криминалист

MediaTek Decrypting Bootloader

- Уязвимые SoC:
  MT6757, MT6755, MT6797, MT6735,
  MT6750, MT6737, MT6753, MT6580
- Для некоторых устройств необходимы подписанные производителем DA и auth файлы

Мобильный Криминалист

Huawei Decrypting Bootloader

- Уязвимые SoC:
  HiSilicon Kirin 92x, 93x, 95x, 96x

Мобильный Криминалист

Извлечение hw-bound key

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

Мобильный Криминалист

http://www.мобильный-криминалист.рф

Извлечение hw-bound key

- Позволяет подбирать пароль вне устройства
- Если подобран пароль или выключена опция Secure Start-Up, то позволяет расшифровать userdata

Мобильный Криминалист

Подходы к расшифровыванию

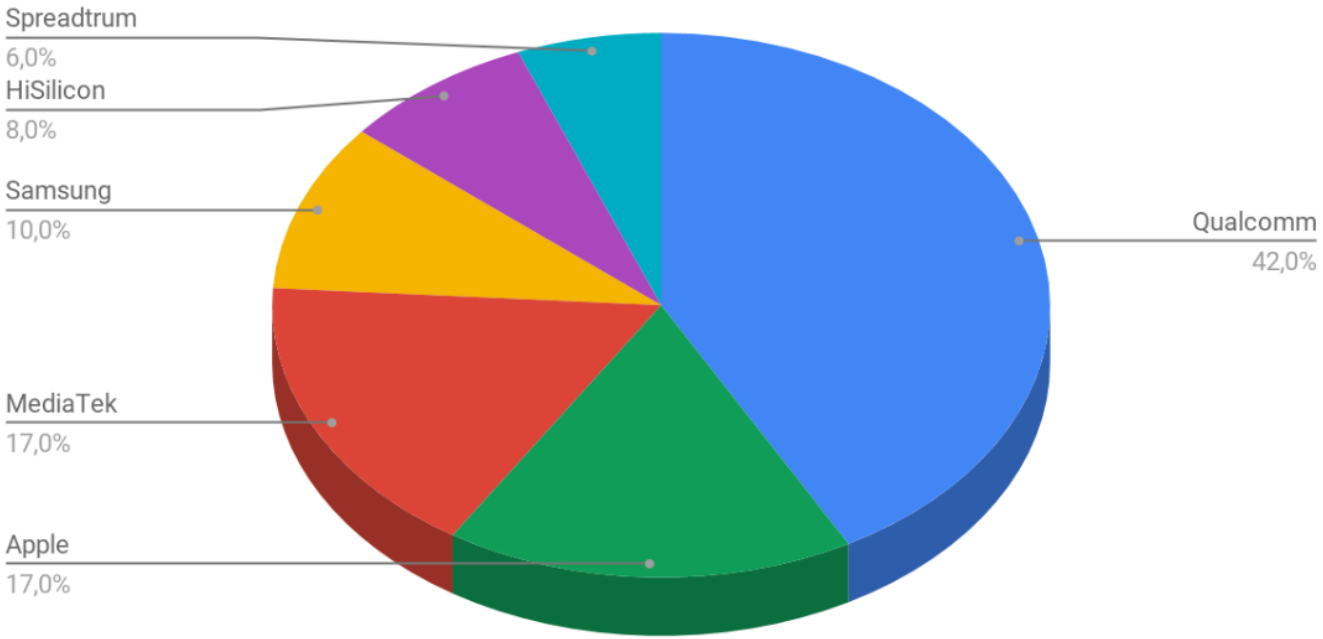
	Внедрение в процесс загрузки	Извлечение hw-bound key
Qualcomm	+	+
MediaTek	+	+
Spreadtrum	*	*
Exynos	+	*
Kirin	+	*

*) На данный момент отсутствует ПО реализующие подход

Мобильный Криминалист

http://www.мобильный-криминалист.рф

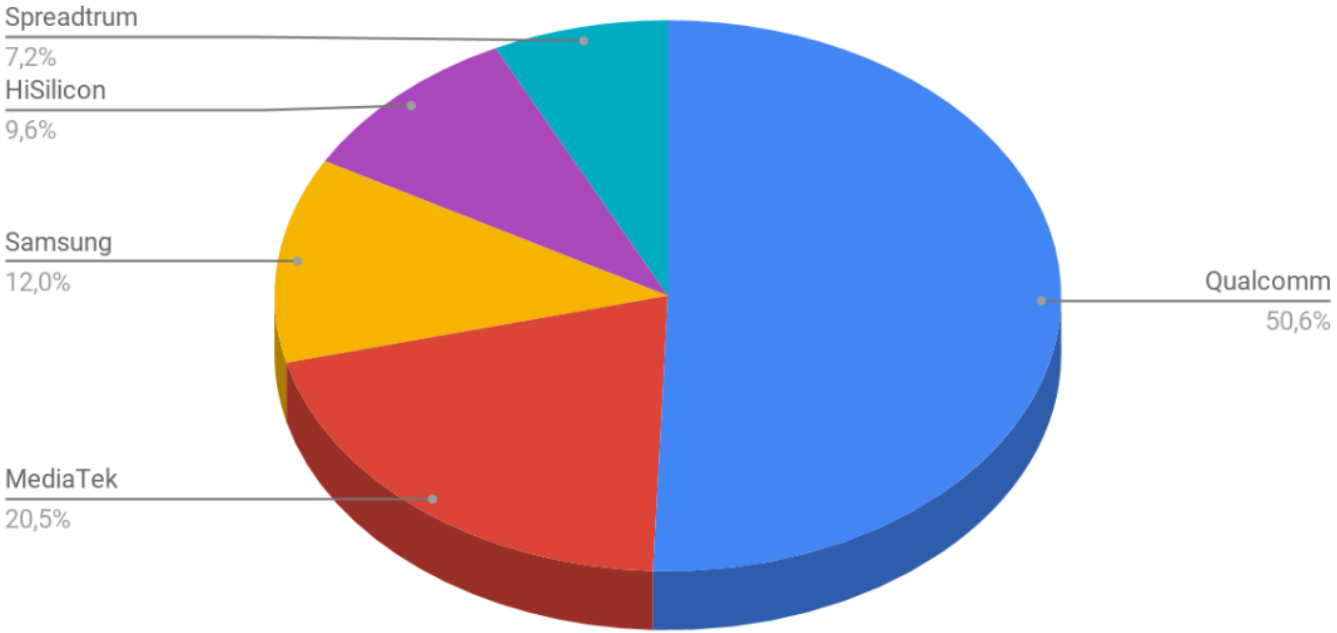
Доля рынка SoC смартфонов



Мобильный Криминалист

http://www.мобильный-криминалист.рф

Доля рынка SoC смартфонов



Мобильный Криминалист

http://www.мобильный-криминалист.рф

Подведем Итоги

- На любом современном Android смартфоне по умолчанию включено шифрование пользовательских данных
- Если включена опция Secure Start-Up, то лучшее что можно сделать – извлечь hw-backed key и пытаться подобрать пароль вне устройства

Мобильный Криминалист

Мобильный Криминалист

Спасибо за внимание!
Вопросы?

Карондеев Андрей Михайлович
karondeev@oxygensoftware.com