Особенности извлечения данных из Samsung Exynos устройств

Карондеев Андрей, специалист отдела исследований мобильных устройств

Оксиджен софтвер

Samsung Exynos

2010
Exynos 3110
45 nm, 1 GHz

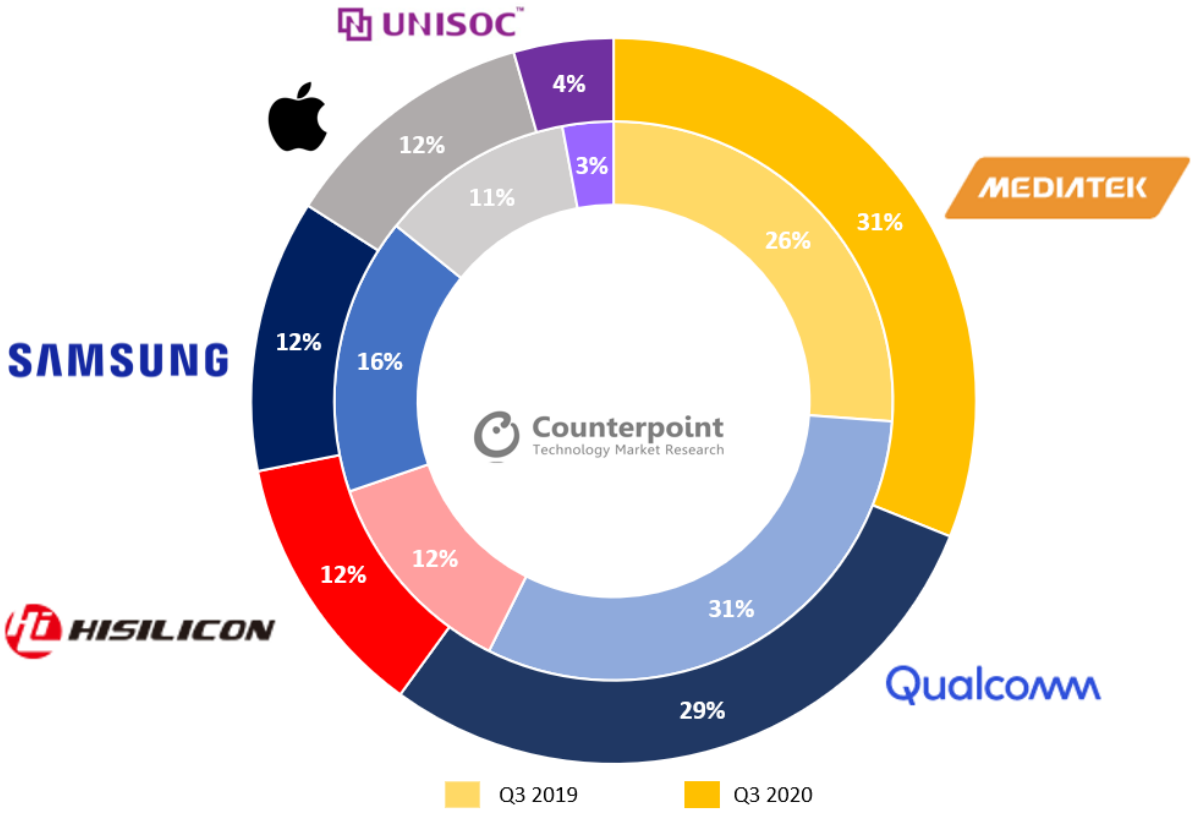
2016
Exynos 8890
14 nm, 2.4 GHz

2021
Exynos 2100
5 nm, 2.9 GHz

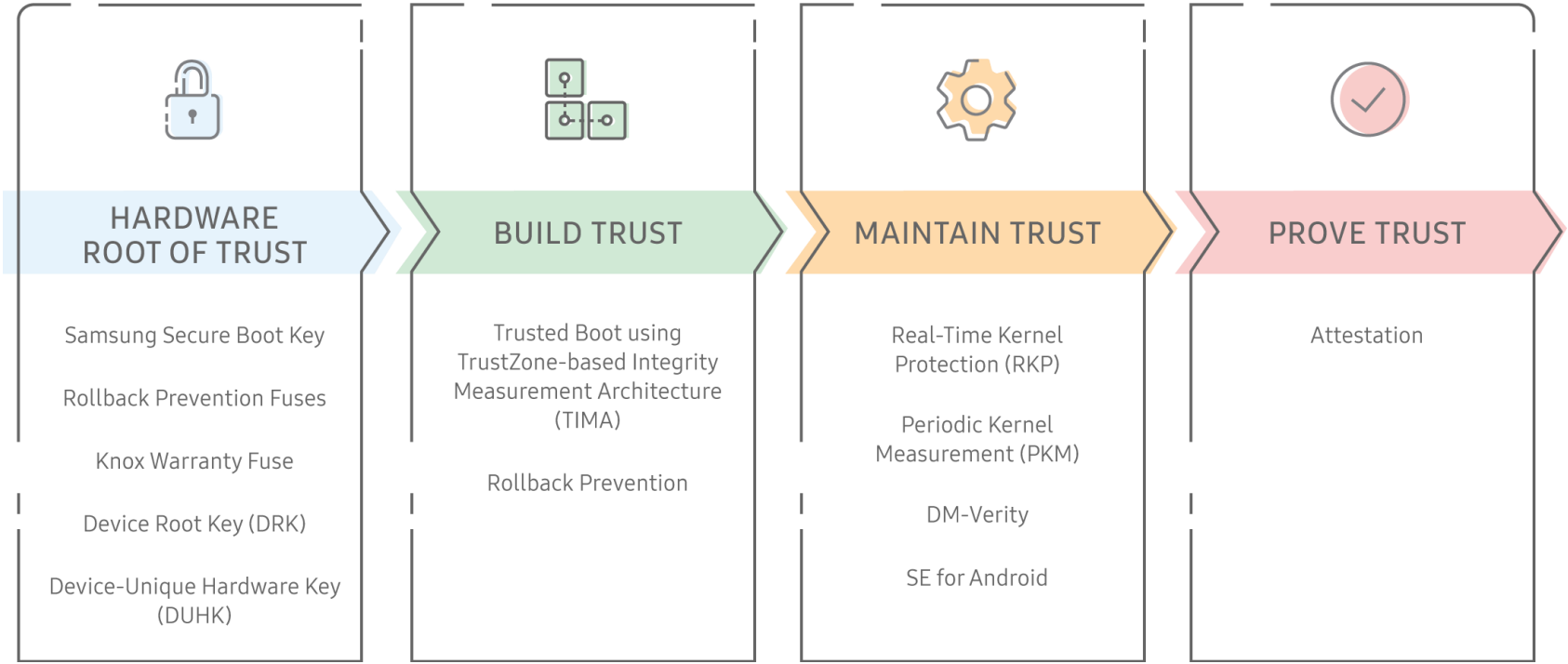
Global Smartphone Shipments Market Share

Brands	2018 Q3	2018 Q4	2019 Q1	2019 Q2	2019 Q3	2019 Q4	2020 Q1	2020 Q2	2020 Q3
Samsung	19%	18%	21%	21%	21%	18%	20%	20%	22%
Huawei	14%	15%	17%	16%	18%	14%	17%	20%	14%
Xiaomi	9%	6%	8%	9%	8%	8%	10%	10%	13%
Apple	12%	17%	12%	10%	12%	18%	14%	14%	11%
Oppo	9%	8%	8%	9%	9%	8%	8%	9%	8%
vivo	8%	7%	7%	8%	8%	8%	7%	8%	8%
realme	–	–	1%	1%	3%	2%	2%	2%	4%
Others	29%	29%	26%	26%	21%	24%	22%	17%	20%

Global Smartphone Chipset Market Share

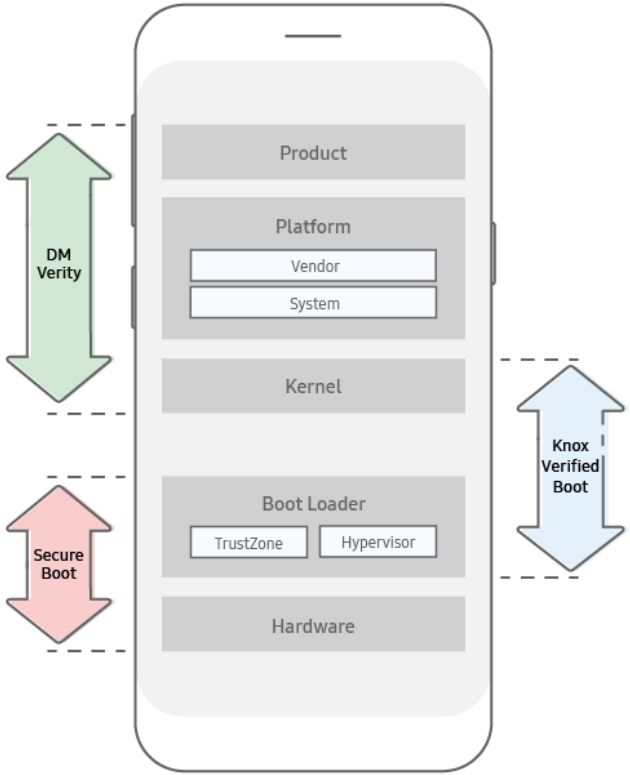


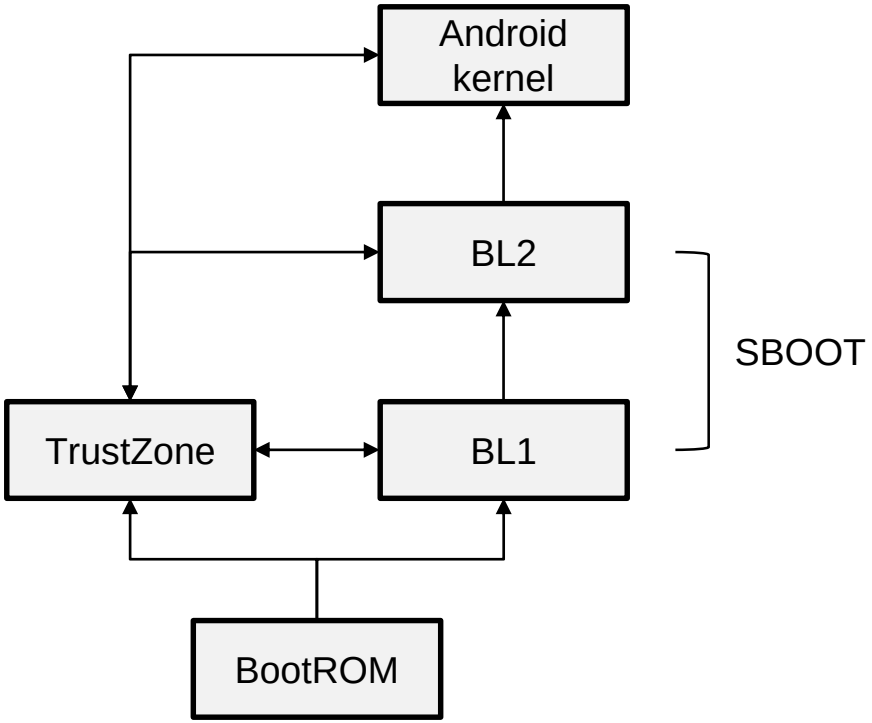
Root of Trust



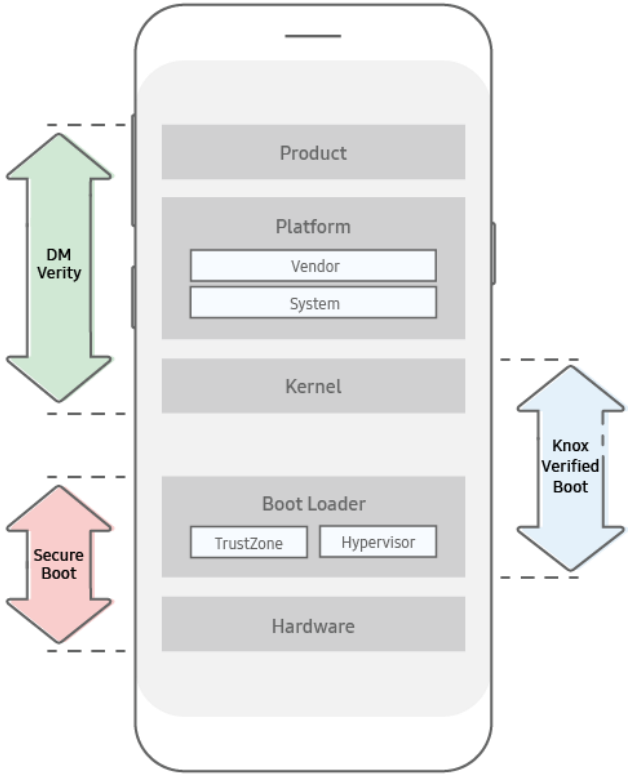
https://docs.samsungknox.com/admin/whitepaper/kpe/hardware-backed-root-of-trust.htm

Samsung Trusted Boot





Samsung Trusted Boot

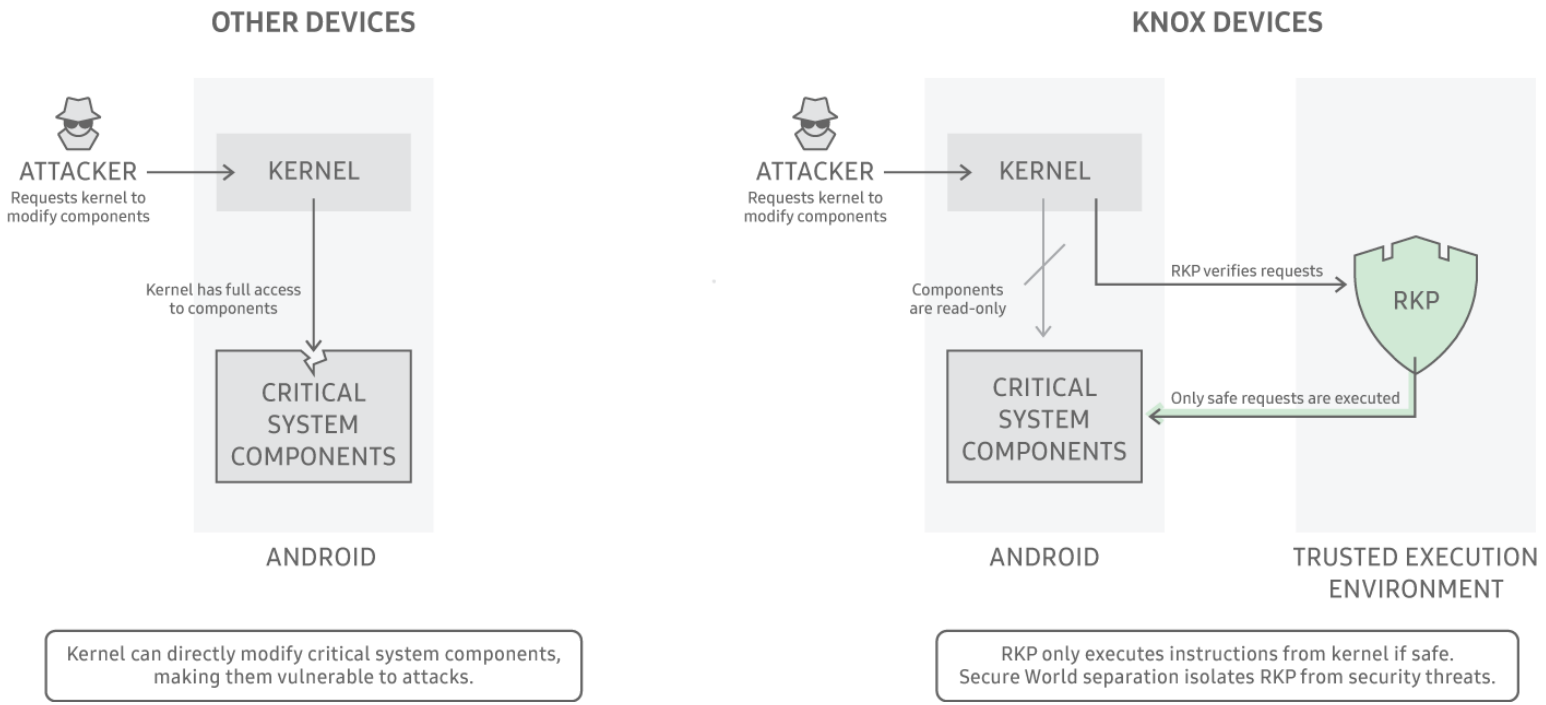


Hardware PBL:
- verify secure boot (SBOOT) & load

SBOOT:
- set handler for Monitor mode, drop privilege
- request EL3 to initial TEEOS
- verify & load hypervisor (uh.bin)
- verify & load kernel (boot.img)

Kernel with DM-Verity:
- verify system.img & mount
- verify vendor.img & mount

Samsung Real-time Kernel Protection (RKP)

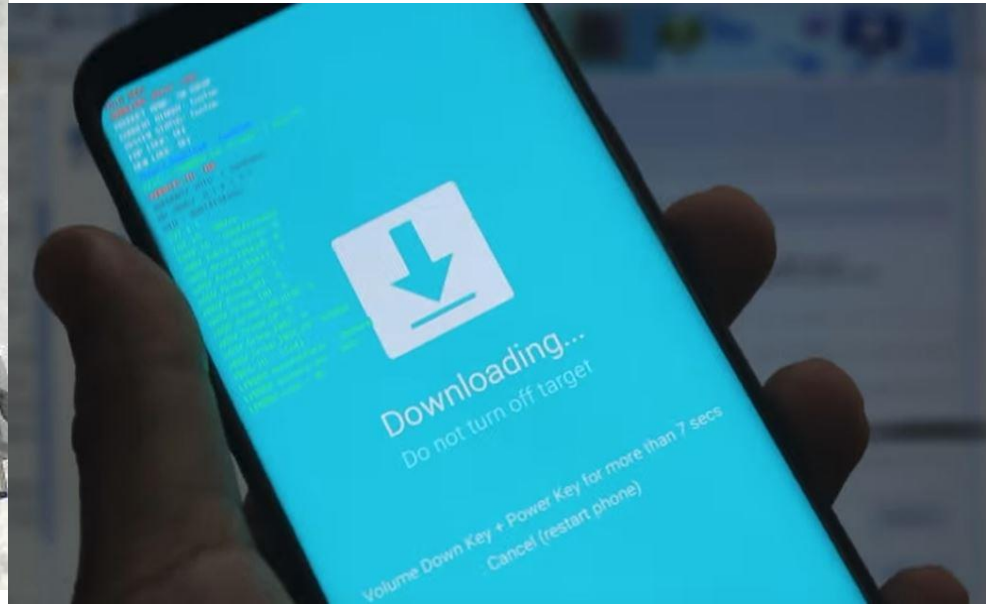


Kernel can directly modify critical system components, making them vulnerable to attacks.

RKP only executes instructions from kernel if safe. Secure World separation isolates RKP from security threats.

Samsung Exynos SBOOT

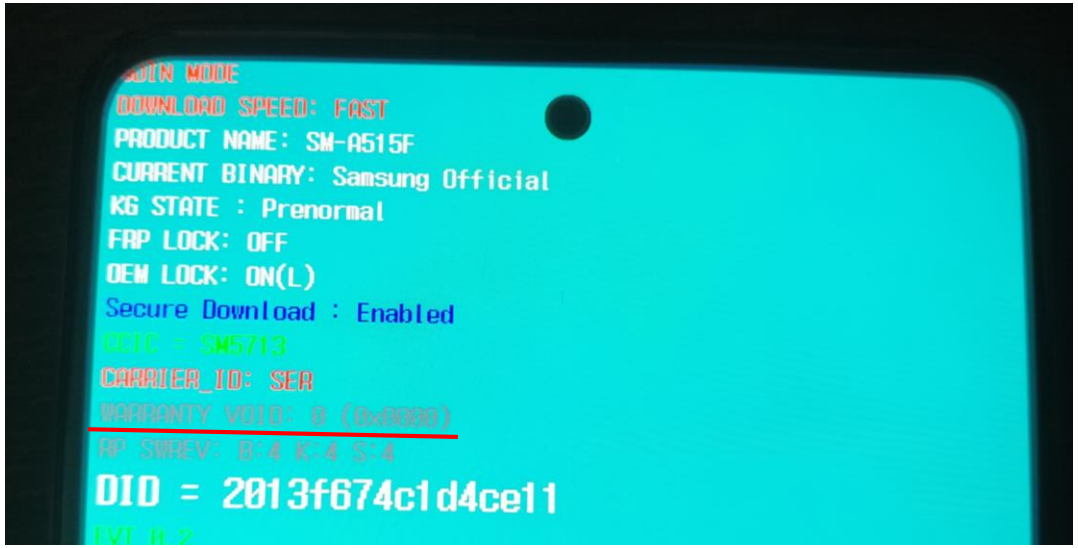
UART Console



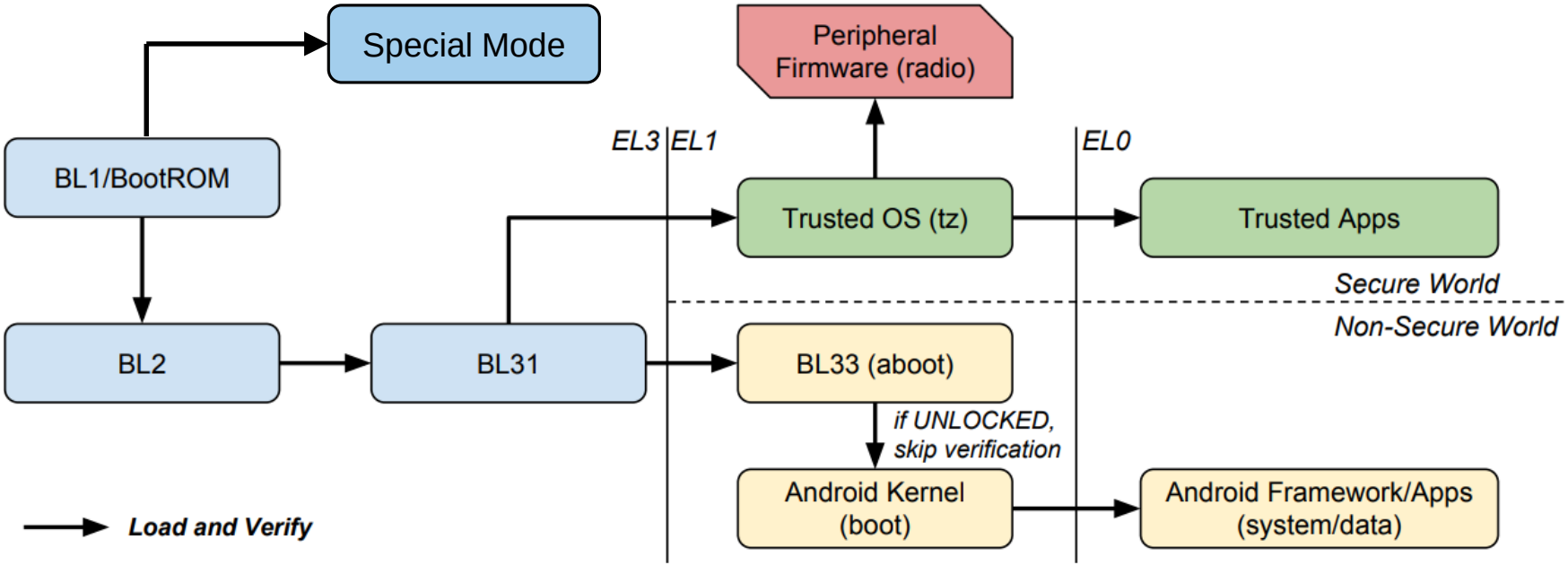
Download Mode

http://hexdetective.blogspot.com/

KNOX WARRANTY VOID

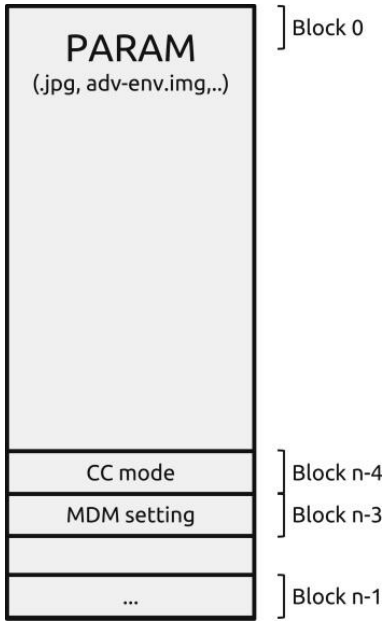


Android boot process



PARAM partition

param.bin
- .jpg boot logo
- adv-env.img
- …



https://www.sciencedirect.com/science/article/pii/S1742287618300409

SBOOT environment variables, stored in adv-env.img

- REBOOT_MODE
- SWITCH_SEL
- DEBUG_LEVEL
- SUD_MODE
- DN_ERROR
- CHECKSUM
- ODIN_DOWNLOAD
- SALES_CODE
- SECURITY_MODE
- NORMAL_BOOT
- CP_DEBUG_LEVEL
- USERBOOT_MODE
- DIAG_MODE
- CHARGING_MODE
- INT_RSVD14
- LCD_RES
- CMDLINE
- BARCODE_INFO
- KEEP_LOG

adv-env.img > CMDLINE

Часовой пояс Оригинальное значение

Извлечения 10

Общие разделы

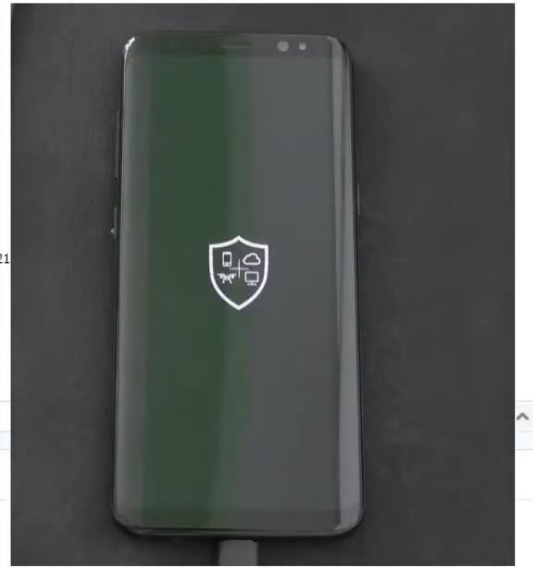
Контакты

Аналитика 4

Важное
245/1

Найти текст...

Время Заметка



Извлечение Samsung Exynos

Извлечение Samsung Exynos

Извлечение данных из устройств Samsung с процессором Exynos.

Подключение устройства

- Поиск устройства Samsung подключенного по USB в режиме ODIN
- Чтение параметров устройства

Устройство обнаружено: Galaxy S8 (SM-G950F) (поддерживается)

Папка извлечения: C:\Users\Marketing\Documents\Oxygen Software\Extractions

Подготовка к извлечению

- Загрузка модифицированного образа в устройство
- Перезагрузка устройства
- Чтение раздела cache (500.0 Mb)
- Загрузка эксплойта в устройство
- Перезагрузка устройства в режиме ODIN
- Применение уязвимости
- Перезагрузка устройства

Пожалуйста перезагрузите устройство в ручном режиме в обычное состояние.
Если устройство перезагрузилось, но не обнаружено в программе, отключите его от ПК и подключите снова.

Извлечение данных

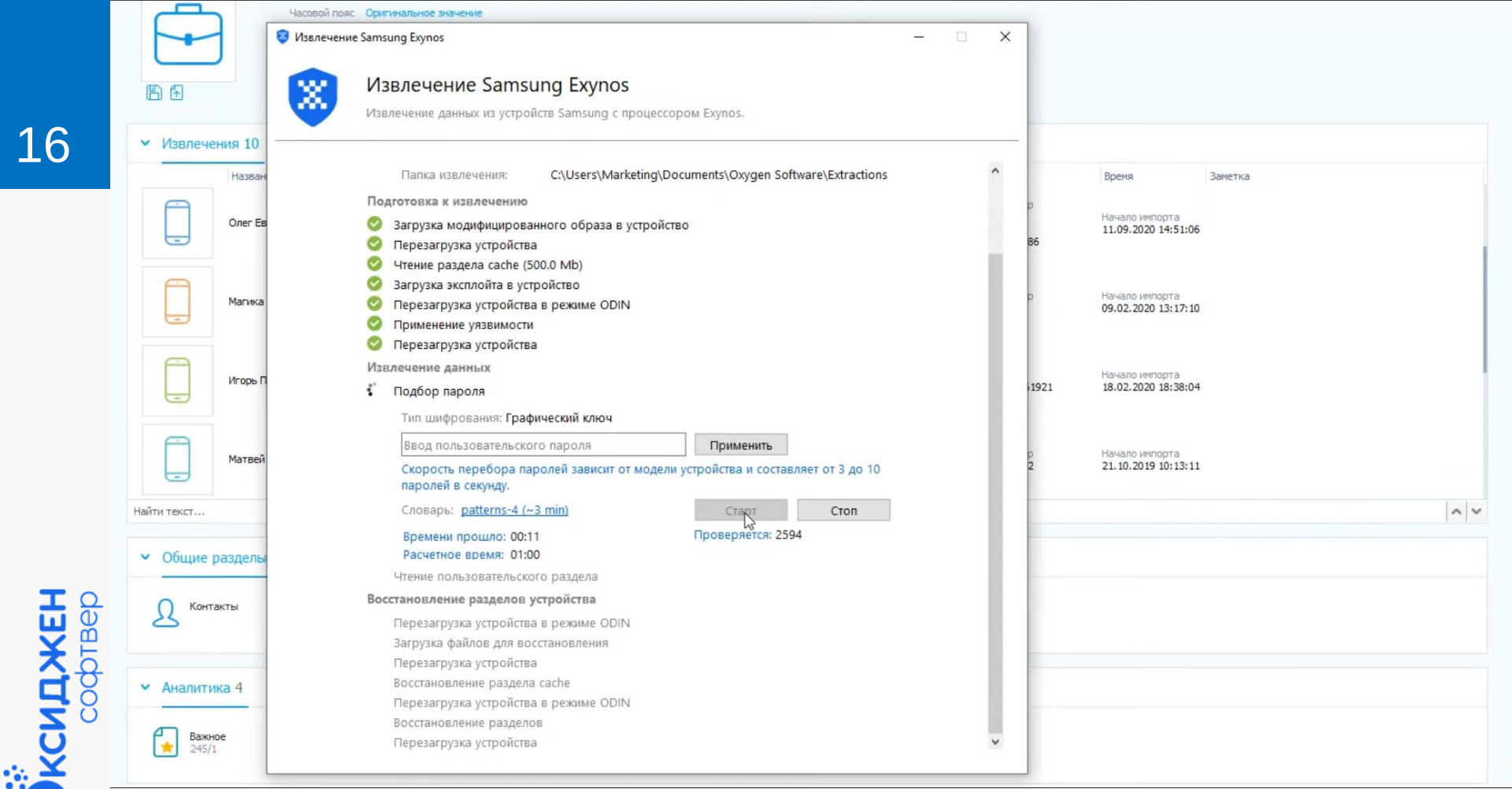
- Подбор пароля
- Чтение пользовательского раздела

Восстановление разделов устройства

- Перезагрузка устройства в режиме ODIN
- Загрузка файлов для восстановления
- Перезагрузка устройства
- Восстановление раздела cache
- Перезагрузка устройства в режиме ODIN
- Восстановление разделов
- Перезагрузка устройства

Оксиджен софтвер

https://youtu.be/ExkCAMPIrAU

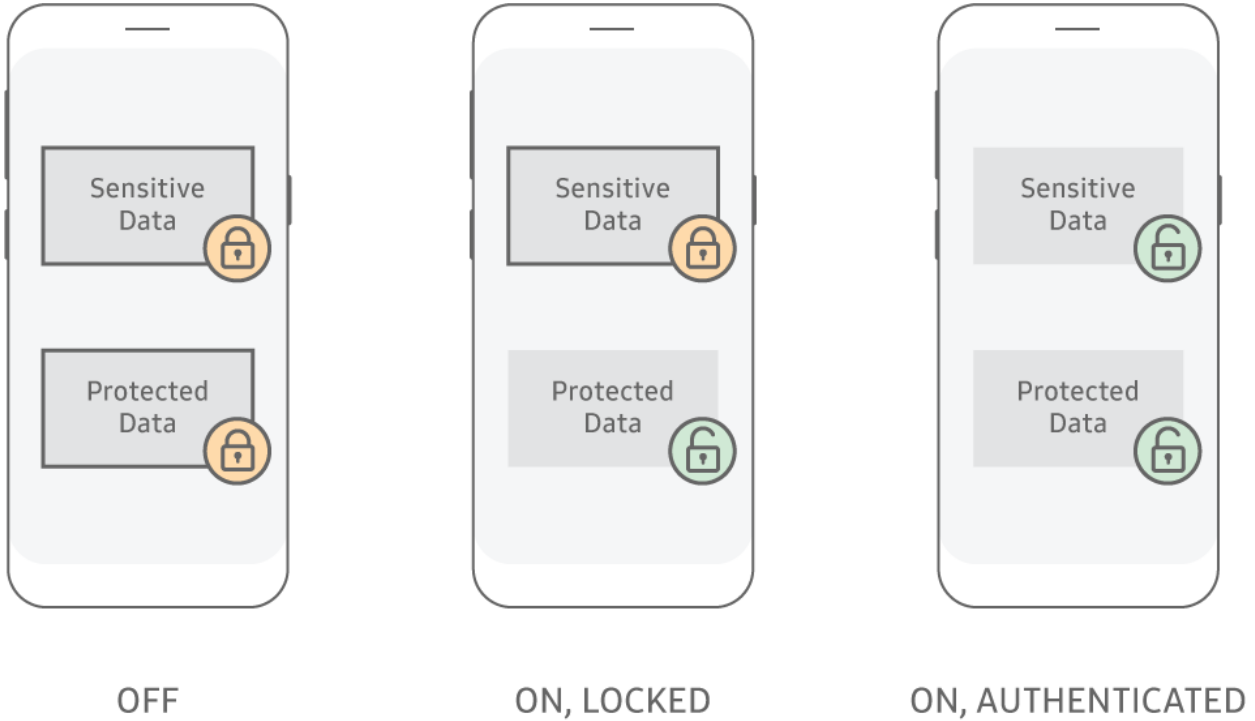


https://youtu.be/ExkCAMPIrAU

Vulnerable devices

Android 7-8 and upgradable to 9
Samsung Exynos devices:
A2-A8, S6-S9, J2-J7

Android 9+ File-Based Encryption



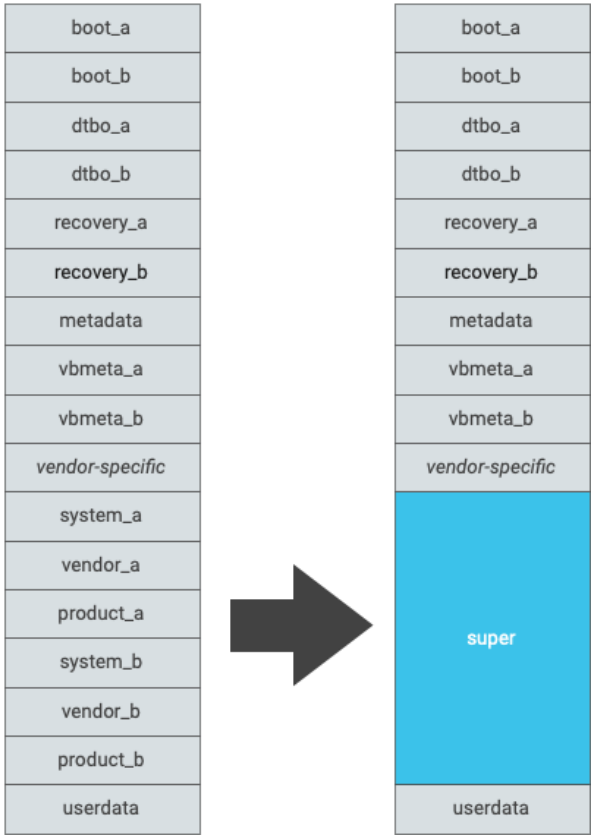
https://docs.samsungknox.com/admin/whitepaper/kpe/sensitive-data-protection.htm

Android 9+ System-as-root (SAR)

Type	Boot Method	Partition	2SI	Ramdisk in `boot`
I	A	A-only	No	`boot` ramdisk
II	B	A/B	Any	`recovery` ramdisk
III	B	A-only	Any	***N/A***
IV	C	Any	Yes	Hybrid ramdisk

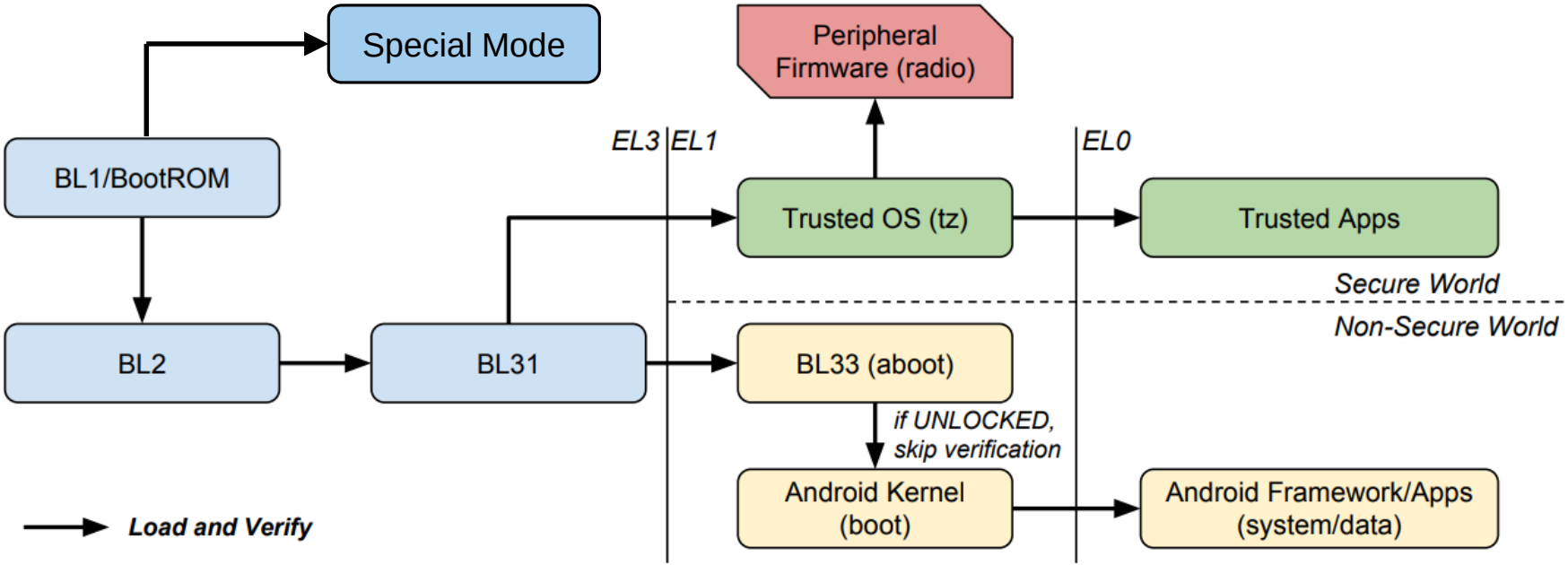
https://topjohnwu.github.io/Magisk/boot.html

Android 10+ Two Stage Init (2SI)



https://source.android.com/devices/tech/ota/dynamic_partitions/implement

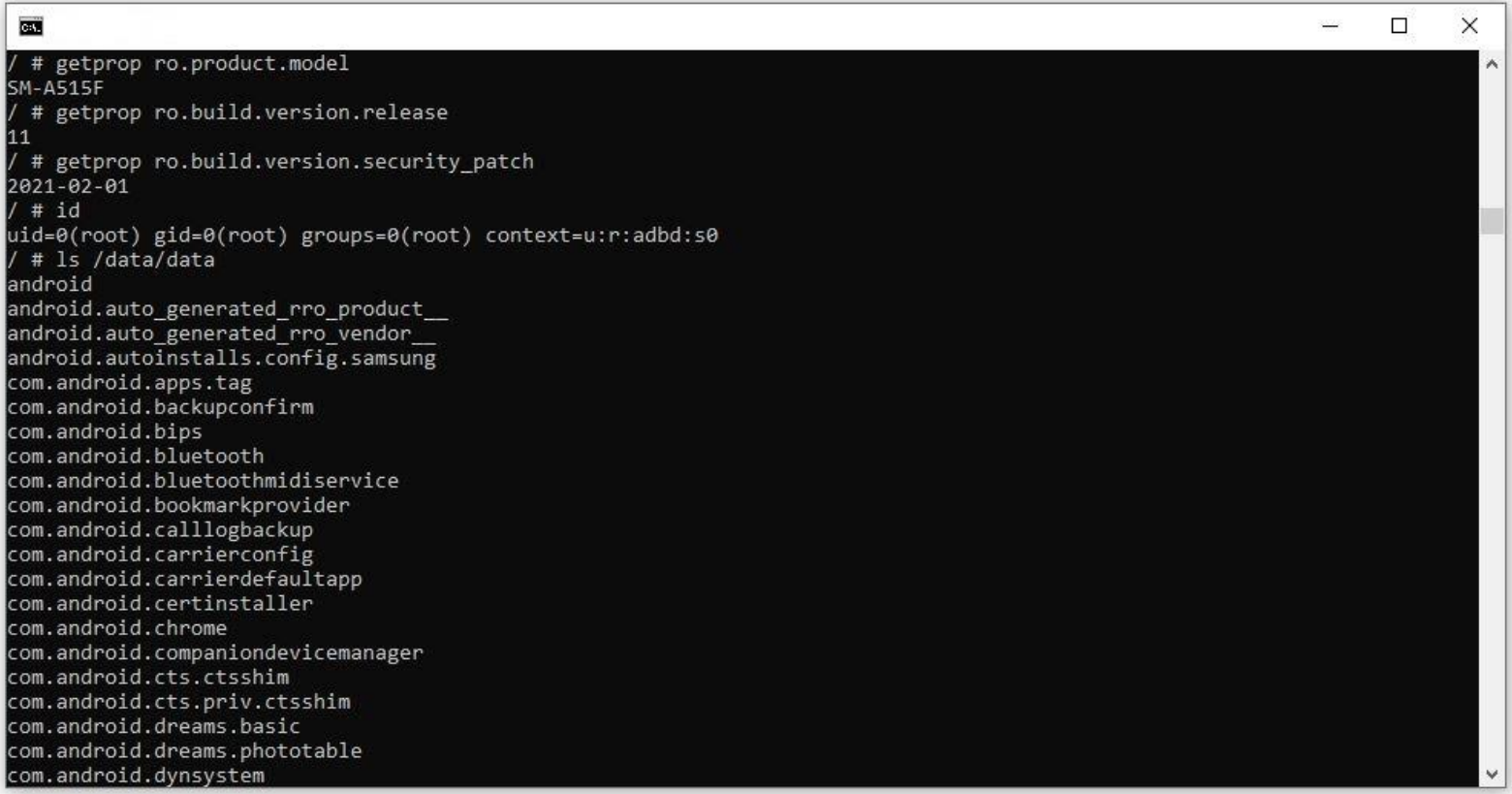
Android 9+ SBOOT Exploit



Android 9+ SBOOT Exploit

- modify CMDLINE
- custom initramfs (ramdisk)
- DEFEX: signed dpolicy
- SELinux: always enforcing

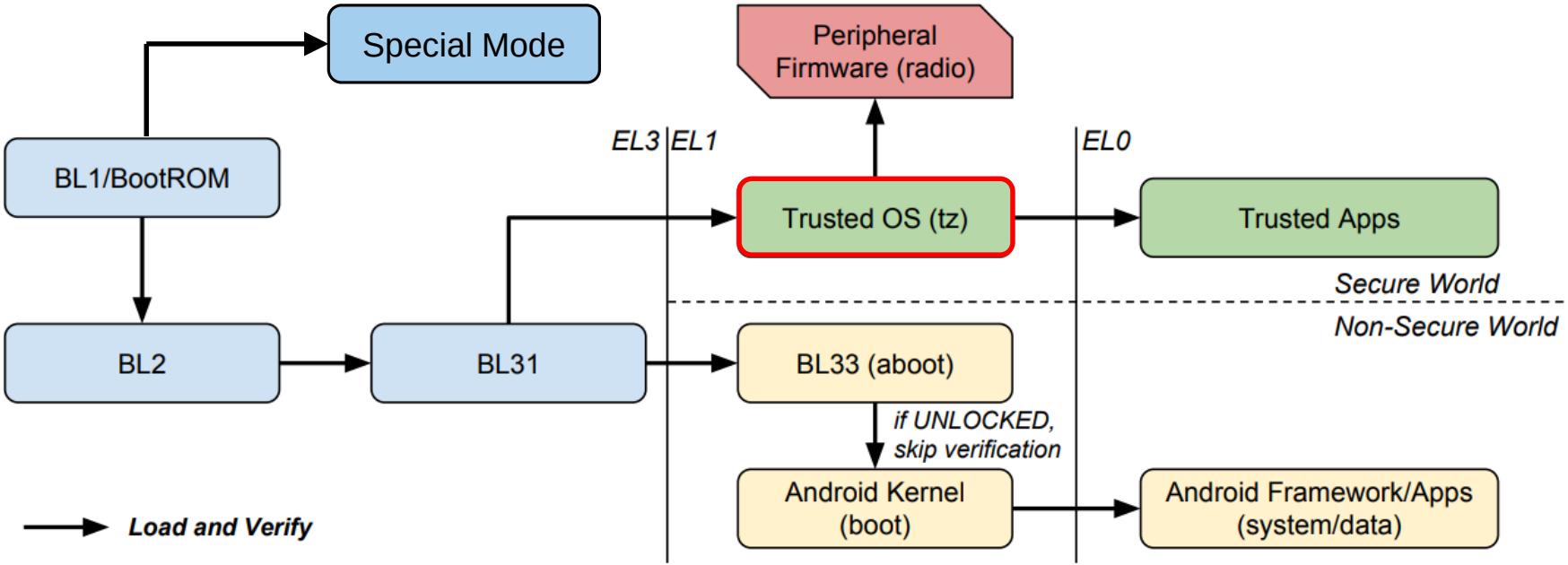
Galaxy A51 (Android 11)



Vulnerable devices

Android 9-11 Samsung Exynos devices:
A10-A51, S10-S20, M10-M31

Breaking Samsung's Root of Trust



https://i.blackhat.com/USA-20/Wednesday/us-20-Chao-Breaking-Samsungs-Root-Of-Trust-Exploiting-Samsung-Secure-Boot.pdf

Подведем Итоги

- Samsung Exynos устройства гораздо лучше защищены от malware в сравнении с большинством других Android устройств
- Тем не менее они содержат уязвимость, позволяющую внедриться в процесс загрузки, которую можно использовать при проведении судебно-технической экспертизы для извлечения данных

Благодарю за внимание!

Карондеев Андрей
karondeev@oxygensoftware.com

Оксиджен софтвер