ARTIFACT EVALUATED usenix ASSOCIATION AVAILABLE

ARTIFACT EVALUATED usenix ASSOCIATION FUNCTIONAL

ARTIFACT EVALUATED usenix ASSOCIATION REPRODUCED

Spill the TeA:

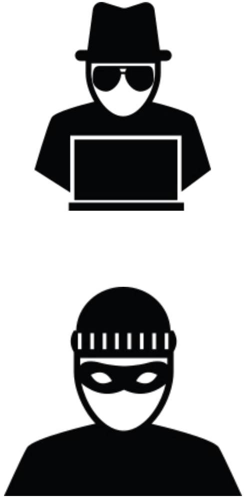
An Empirical Study of Trusted Application Rollback Prevention on Android Smartphones

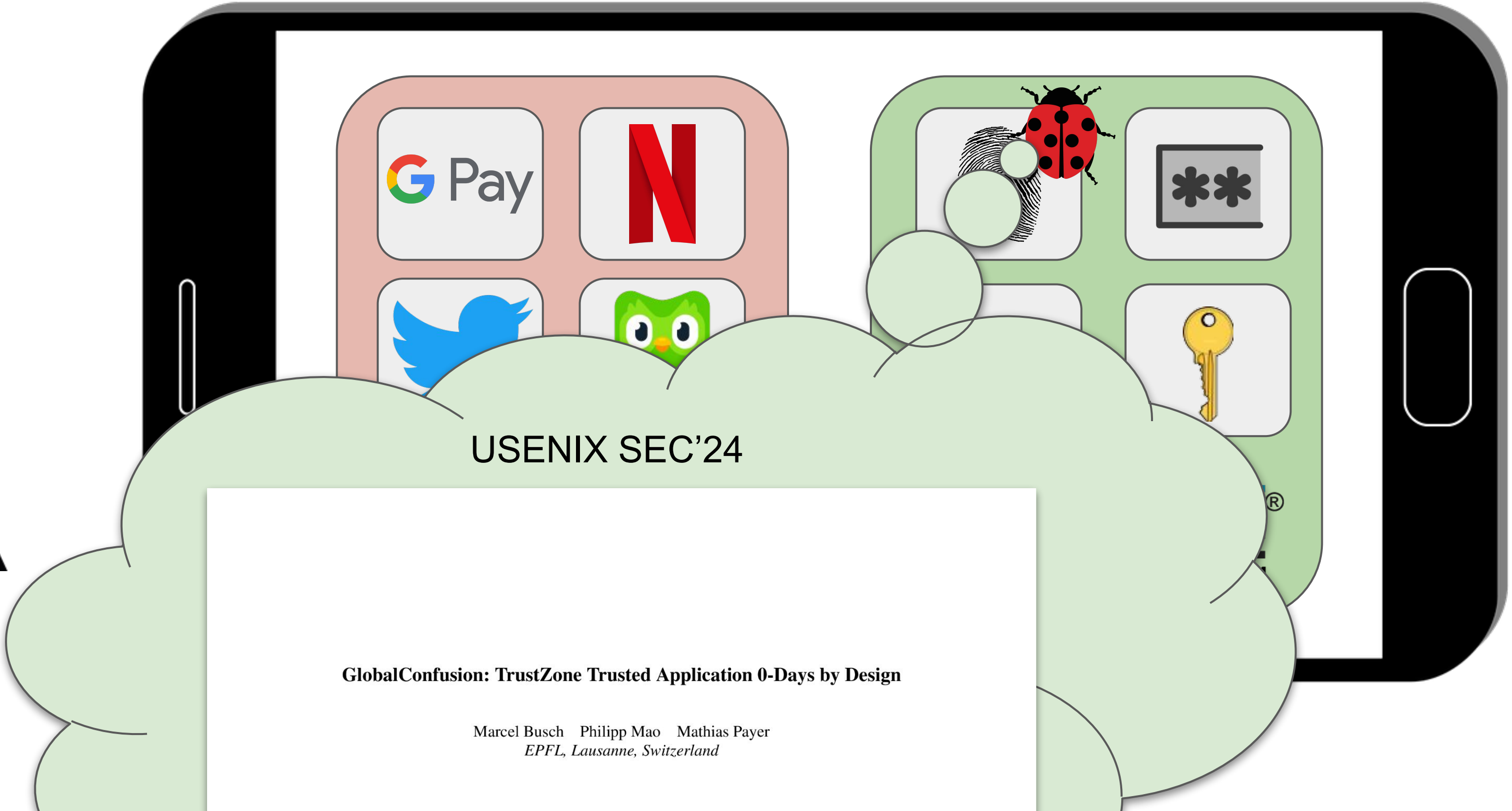
Marcel Busch, Philipp Mao, Mathias Payer
EPFL, Lausanne, Switzerland

HexHive

EPFL

Trusted Applications on Mobile Devices

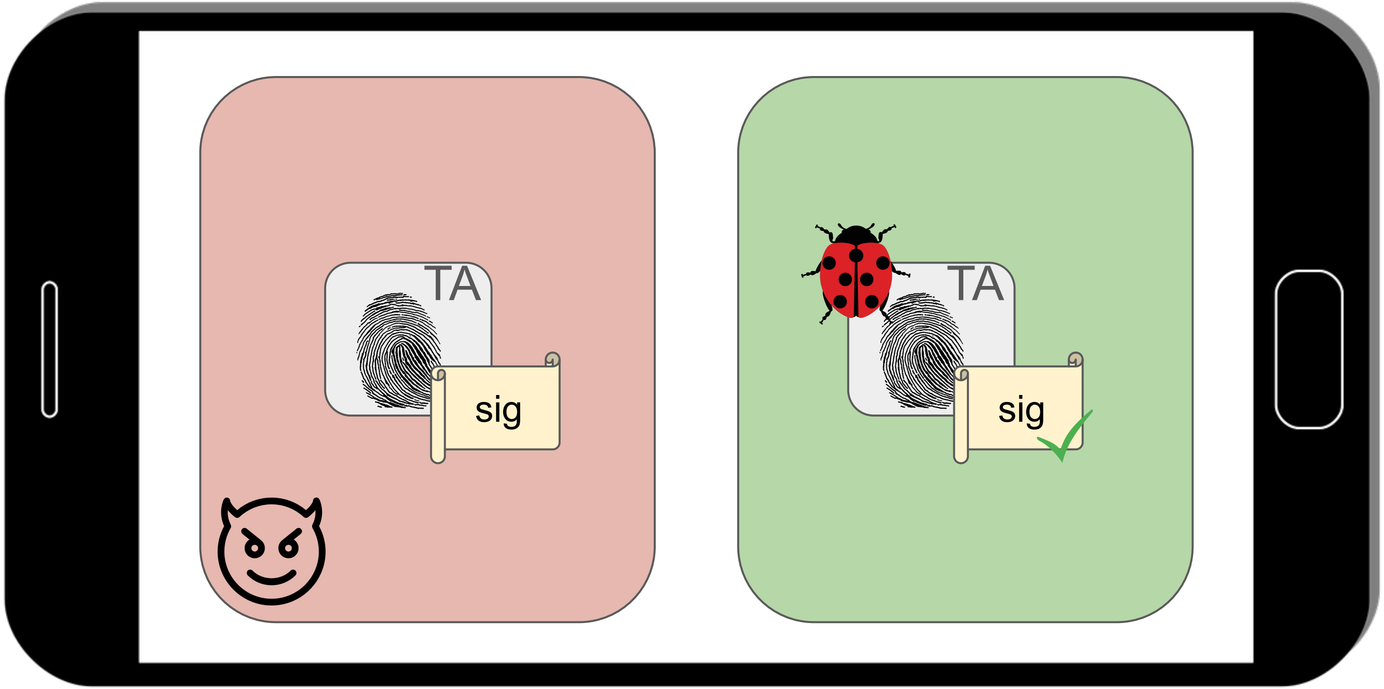




GlobalConfusion: TrustZone Trusted Application 0-Days by Design

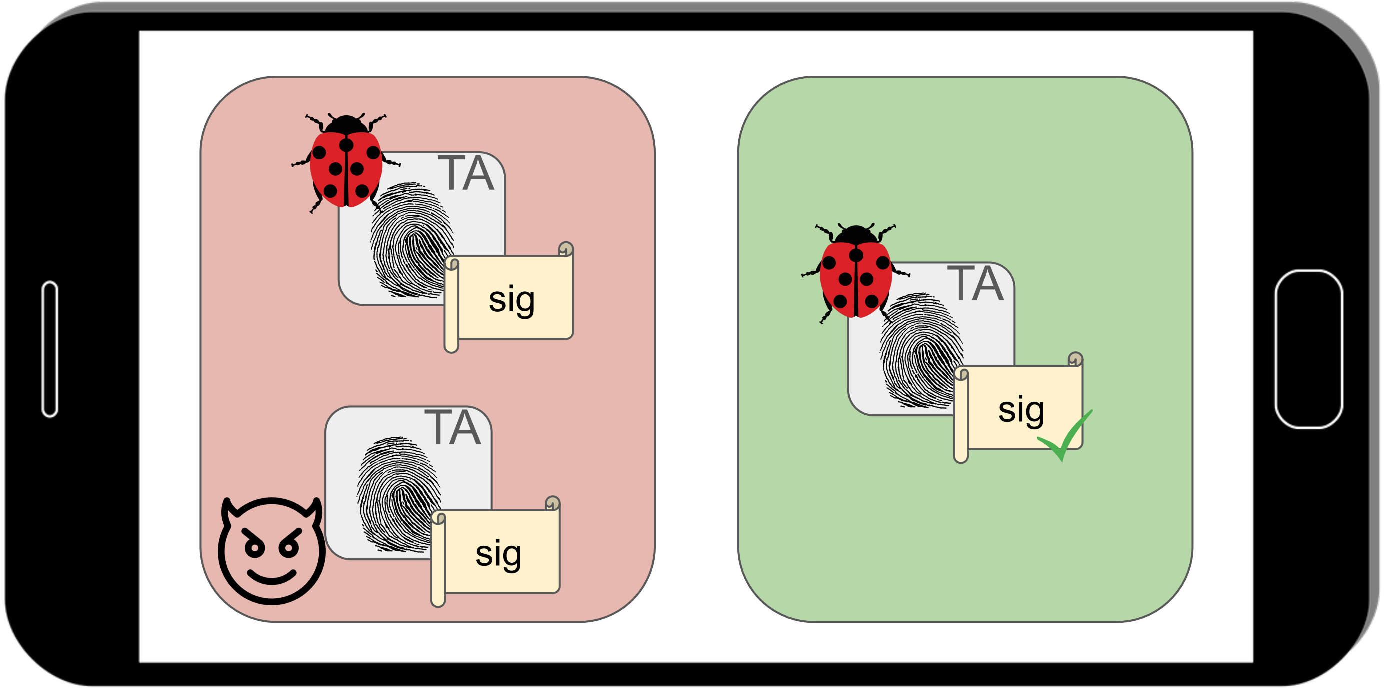
Marcel Busch Philipp Mao Mathias Payer
EPFL, Lausanne, Switzerland

Trusted Applications



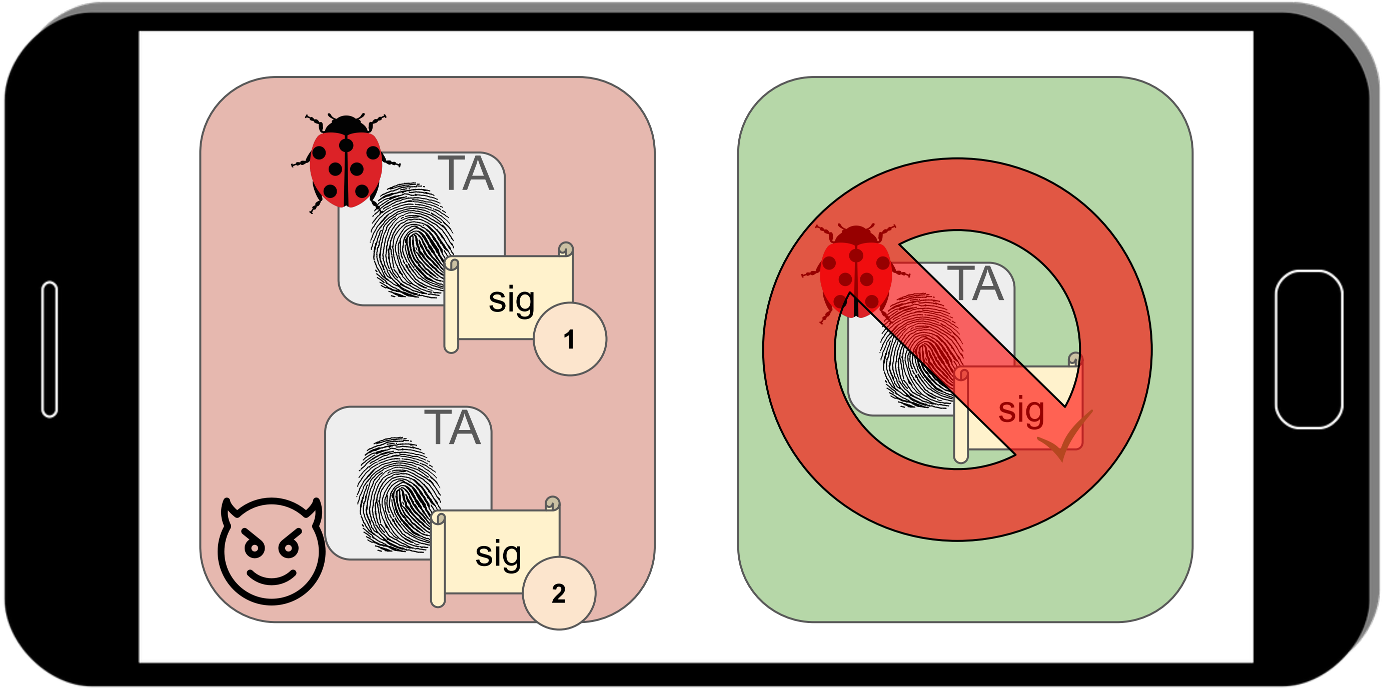
Trusted Applications are authentic dynamically-loadable modules

TA Rollback Attacks



TA Rollback Attacks exploit the authenticity of old and vulnerable TAs

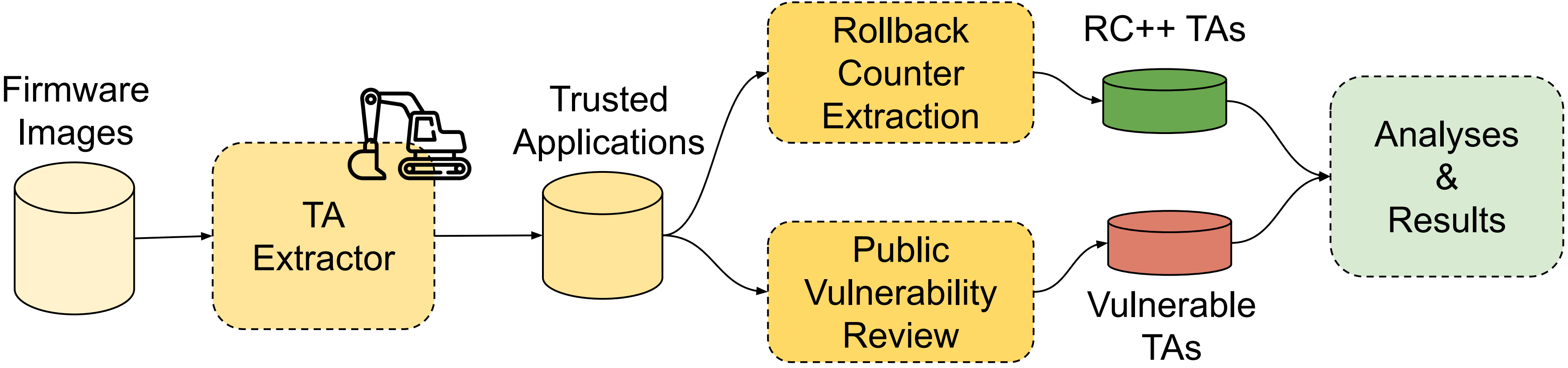
TA Rollback Prevention



TA Rollback Counters allow TEEs to stick to the latest known TA version

Empirical Study

Overview



5 OEMs >65% market share

focus on last 4y

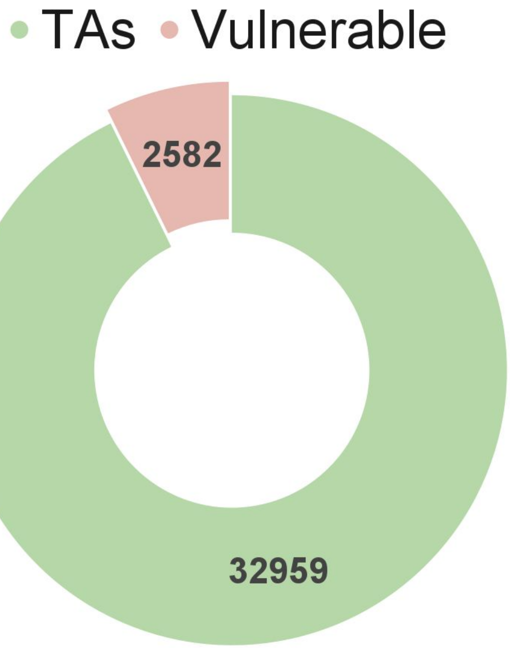
>= 5 firmware images per phone

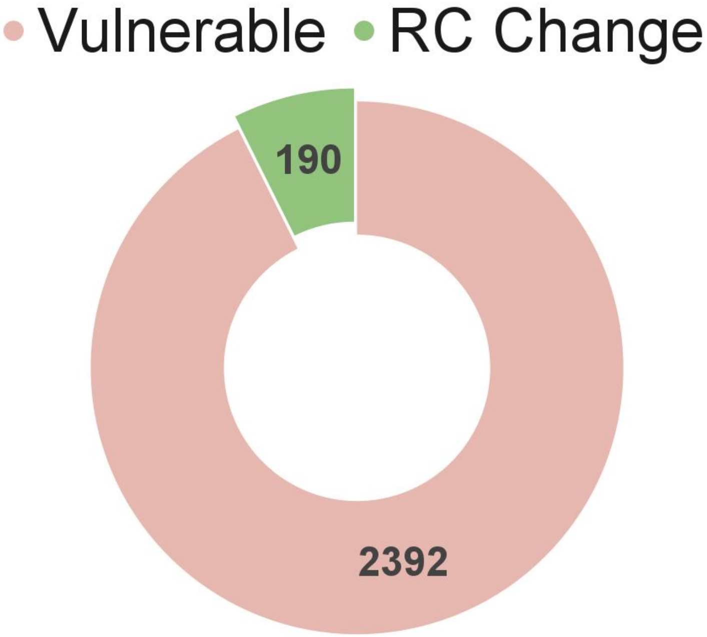
~ 35,500 TAs (293 unique)
4 TEEs

190 rollback counter events

~ 2,500 vulnerable TAs

Rollback Counter Usage Overview

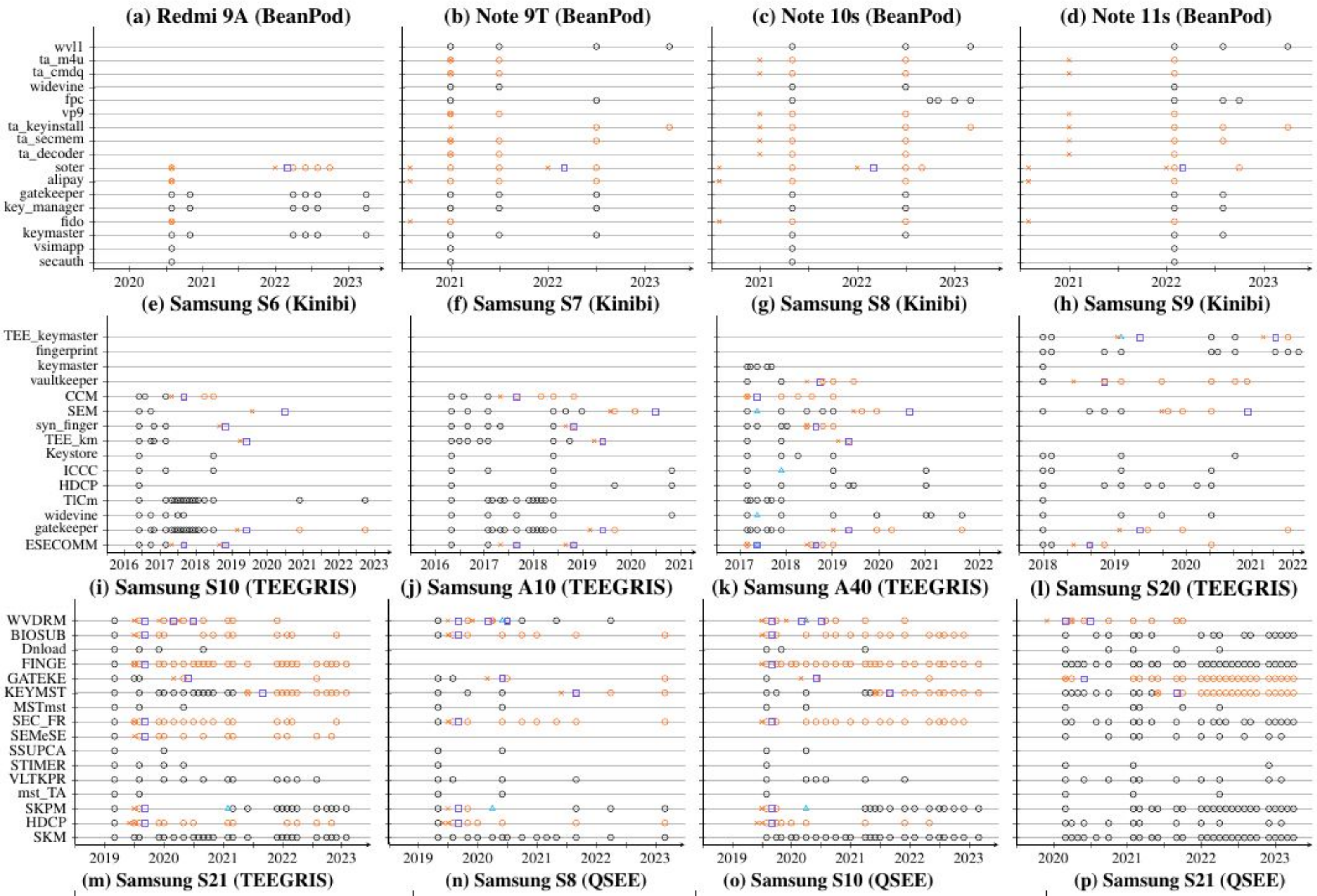




RCs not used although **public** vulnerability advisories exist

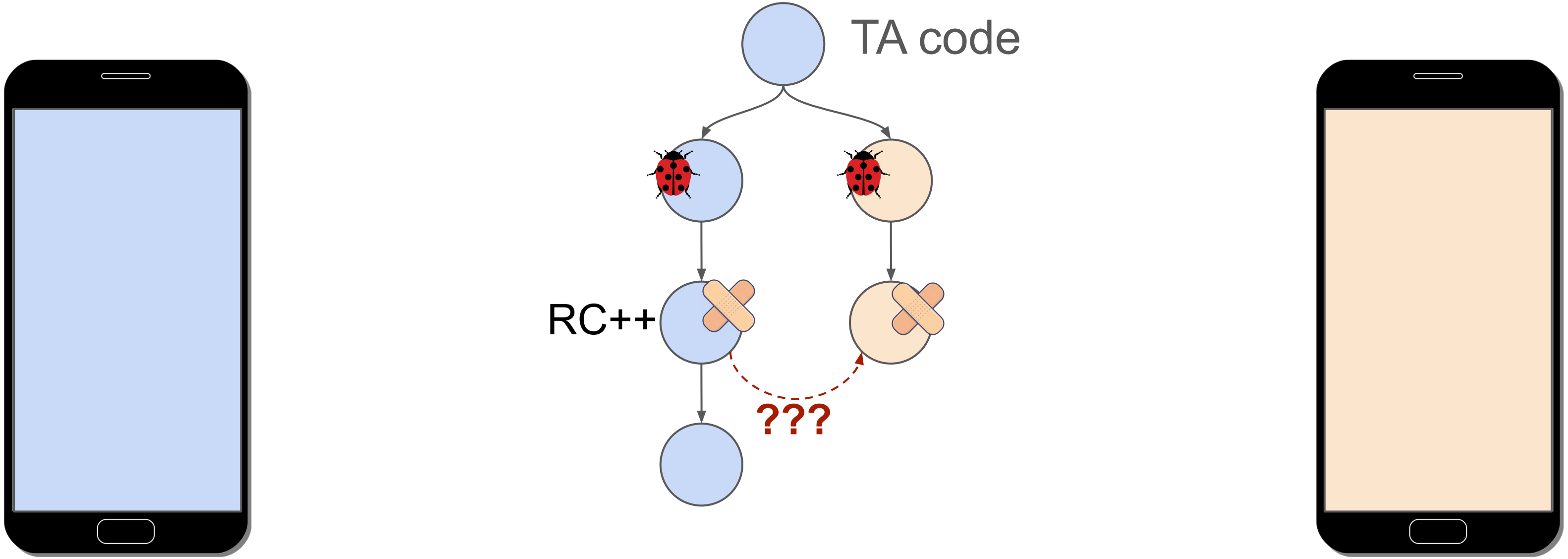
TA rollback affects 29 out of 51 devices

Only vendor with RC changes is Samsung


(a) Redmi 9A (BeanPod)
(b) Note 9T (BeanPod)
(c) Note 10s (BeanPod)
(d) Note 11s (BeanPod)
wvl1
ta_m4u
ta_cmdq
widevine
fpc
vp9
ta_keyinstall
ta_secmem
ta_decoder
soter
alipay
gatekeeper
key_manager
fido
keymaster
vsimapp
secauth
2020
2021
2022
2023
(e) Samsung S6 (Kinibi)
(f) Samsung S7 (Kinibi)
(g) Samsung S8 (Kinibi)
(h) Samsung S9 (Kinibi)
TEE_keymaster
fingerprint
keymaster
vaultkeeper
CCM
SEM
syn_finger
TEE_km
Keystore
ICCC
HDCP
TlCm
widevine
gatekeeper
ESECOMM
2016
2017
2018
2019
2020
2021
2022
2023
(i) Samsung S10 (TEEGRIS)
(j) Samsung A10 (TEEGRIS)
(k) Samsung A40 (TEEGRIS)
(l) Samsung S20 (TEEGRIS)
WVDRM
BIOSUB
Dnload
FINGE
GATEKE
KEYMST
MSTmst
SEC_FR
SEMeSE
SSUPCA
STIMER
VLTKPR
mst_TA
SKPM
HDCP
SKM
2019
2020
2021
2022
2023
(m) Samsung S21 (TEEGRIS)
(n) Samsung S8 (QSEE)
(o) Samsung S10 (QSEE)
(p) Samsung S21 (QSEE)

TA Rollback Counter Caveats

X-Product Leakage



Product of Corp A

Samsung A10

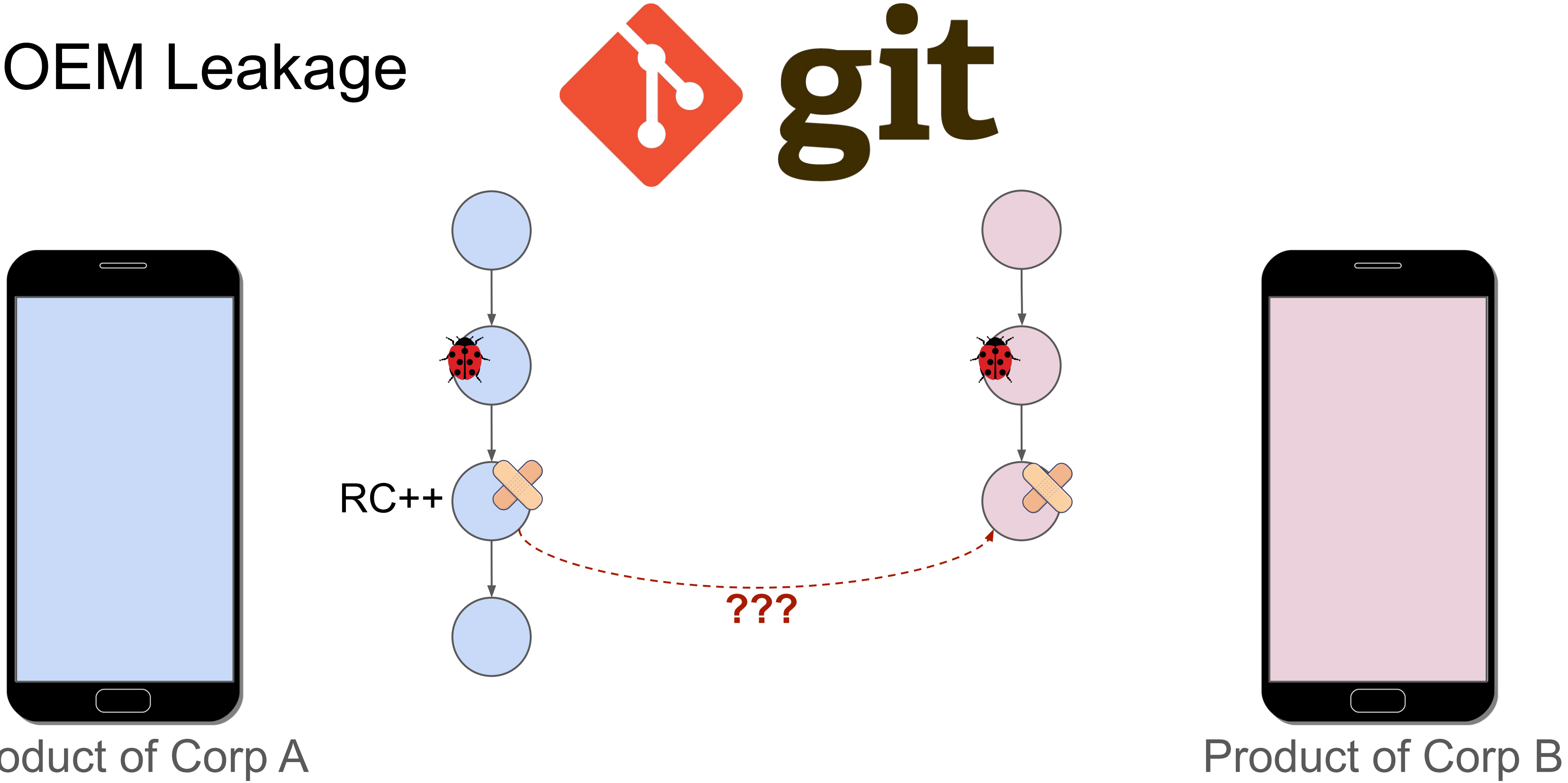
Widevine TA

Samsung Galaxy S10

Product of Corp A

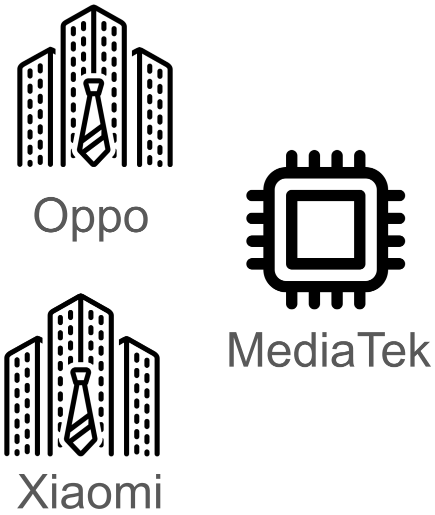
Uncoordinated TA Rollback Counter increments can threaten **other products**

X-OEM Leakage



Uncoordinated TA Rollback Counter increment can threaten **other OEMs**

Uncoordinated Rollback Counter Increments (cont.)



Oppo

Vivo

MediaTek

Xiaomi

14 shared TAs
(some vulnerable)

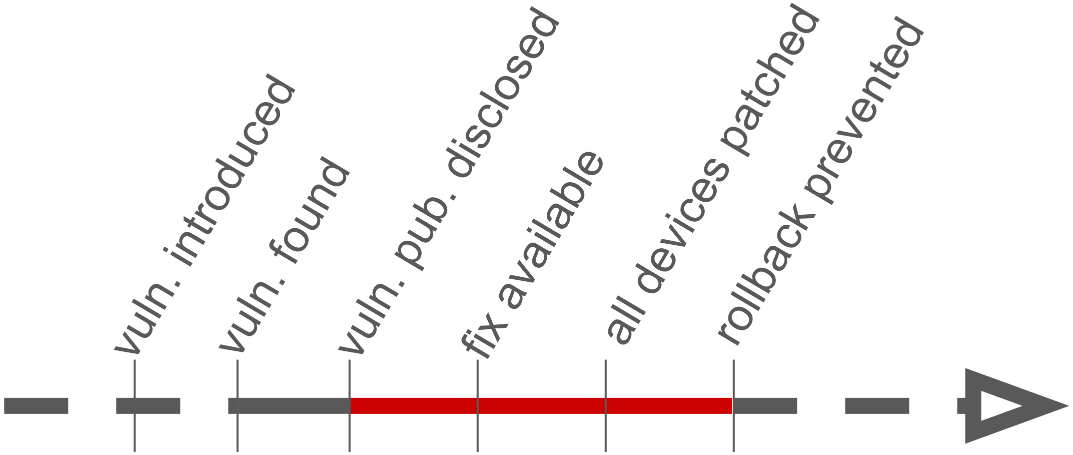
no TA rollback counter

OEMs run the same ODM TA code on their devices

Conclusions

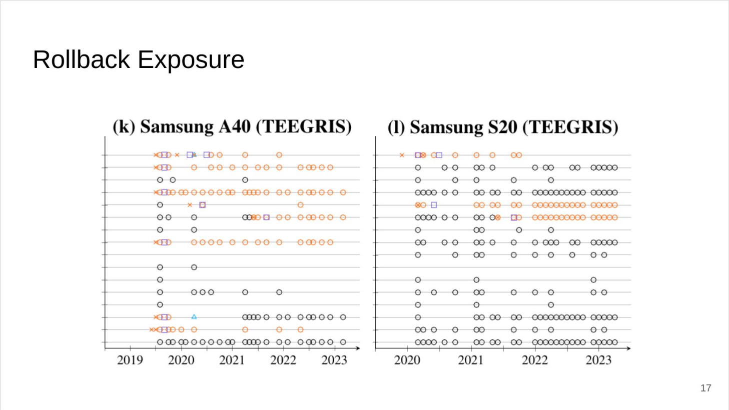
Takeaways

- TA rollback prevention is ineffective at an industry-wide scale
- Questionable TA vulnerability practices
  - No capability for rollback counters
  - Uncoordinated usage of rollback counters
- Lack of transparency regarding TA rollback prevention



Spill the TeA: An Empirical Study of Trusted Application Rollback Prevention on Android Smartphones

Modern TZ-based TEEs on Android Mobile Devices



Rollback Exposure

Paper

Code

ARTIFACT EVALUATED usenix ASSOCIATION AVAILABLE

ARTIFACT EVALUATED usenix ASSOCIATION FUNCTIONAL

ARTIFACT EVALUATED usenix ASSOCIATION REPRODUCED

marcel.busch@epfl.ch

𝕏@0ddc0de

EPFL

This presentation has been designed using resources from Flaticon.com