OpenDTeX – Linux Secure Boot

31C3

Frédéric Guihéry

AMOSSYS

Evil Maid Attack ?

Evil Mail Attack Scenario

Evil maid

FDE protected laptop

Innocent business guy

Evil Mail Attack Scenario

1. FDE protected laptop left in the hotel room
2. Maid installs a malware that exposes a fake passphrase form UI (and clean the room)
3. Laptop owner gets back and types in his passphrase
4. Passphrase is either exfiltrated or stored locally by the malware
5. A bit later, maid steals the laptop and retrieves the decrypted content

The problem: how to trust your laptop ?

OpenDTeX Project

OpenDTeX: Research Project

French « RAPID » grant

Two objectives

- User trust in its operating system
- Protected execution of sensitive code

Contributions

- Secure Boot
- Secure Enclave

Partners

- AMOSSYS
- Bertin Technologies
- Telecom Paristech

Focus on OpenDTeX Secure Boot

OpenDTeX Secure Boot

Objectives

- Integrity verification at OS launch time
- Integrity proof towards a user/remote platform

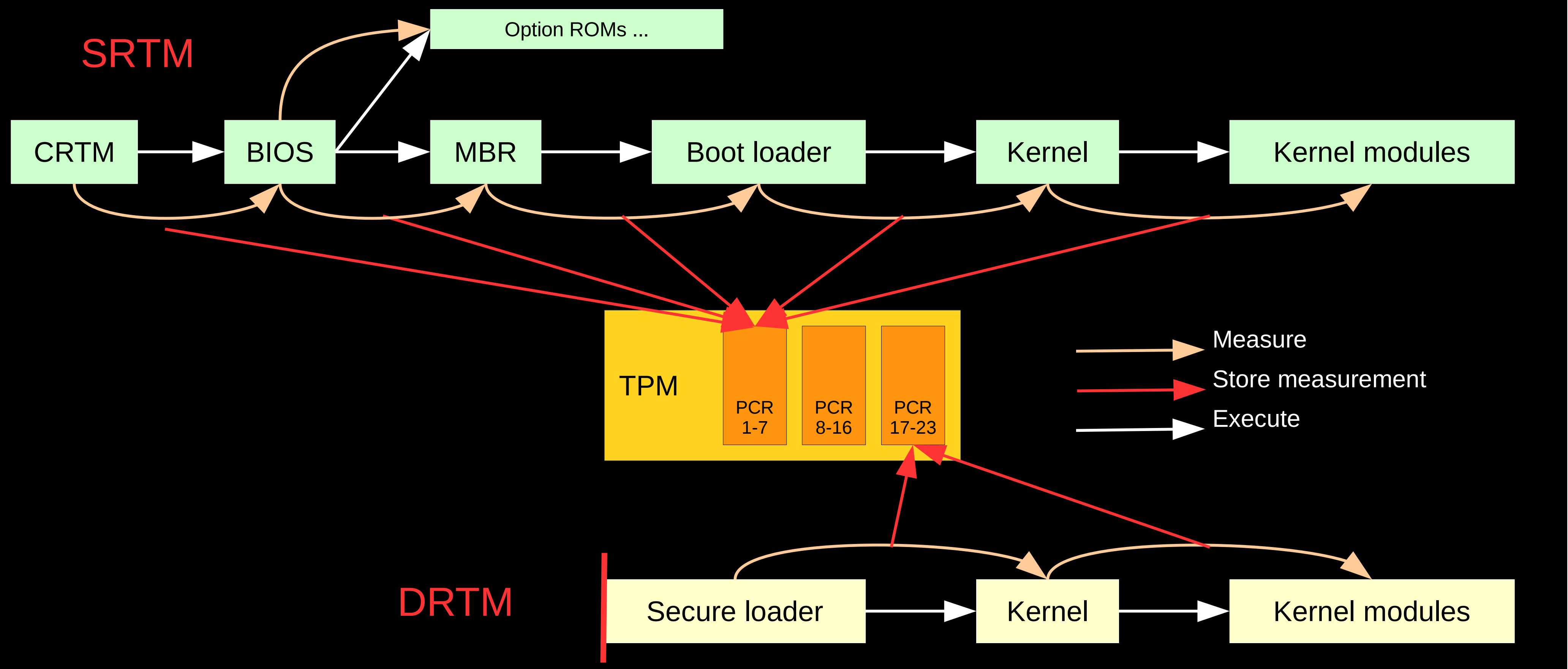
Integrity Proofs

Local proof types

- Implicit local attestation
  - Conditional unsealing of the OS
- Explicit local attestation
  - Secret banner (text or image) only known from the user and conditionaly unsealed
- Explicit remote (but still local) attestation
  - Attestion on Android smartphone via USB (see Android-attest PoC @ SSTIC 2013 by Tibapbedoum)

Secure Boot Architecture ?

Reminder on Chain of Trust



Hardware requirements

SRTM use case

- TPM – Cryptographic provider

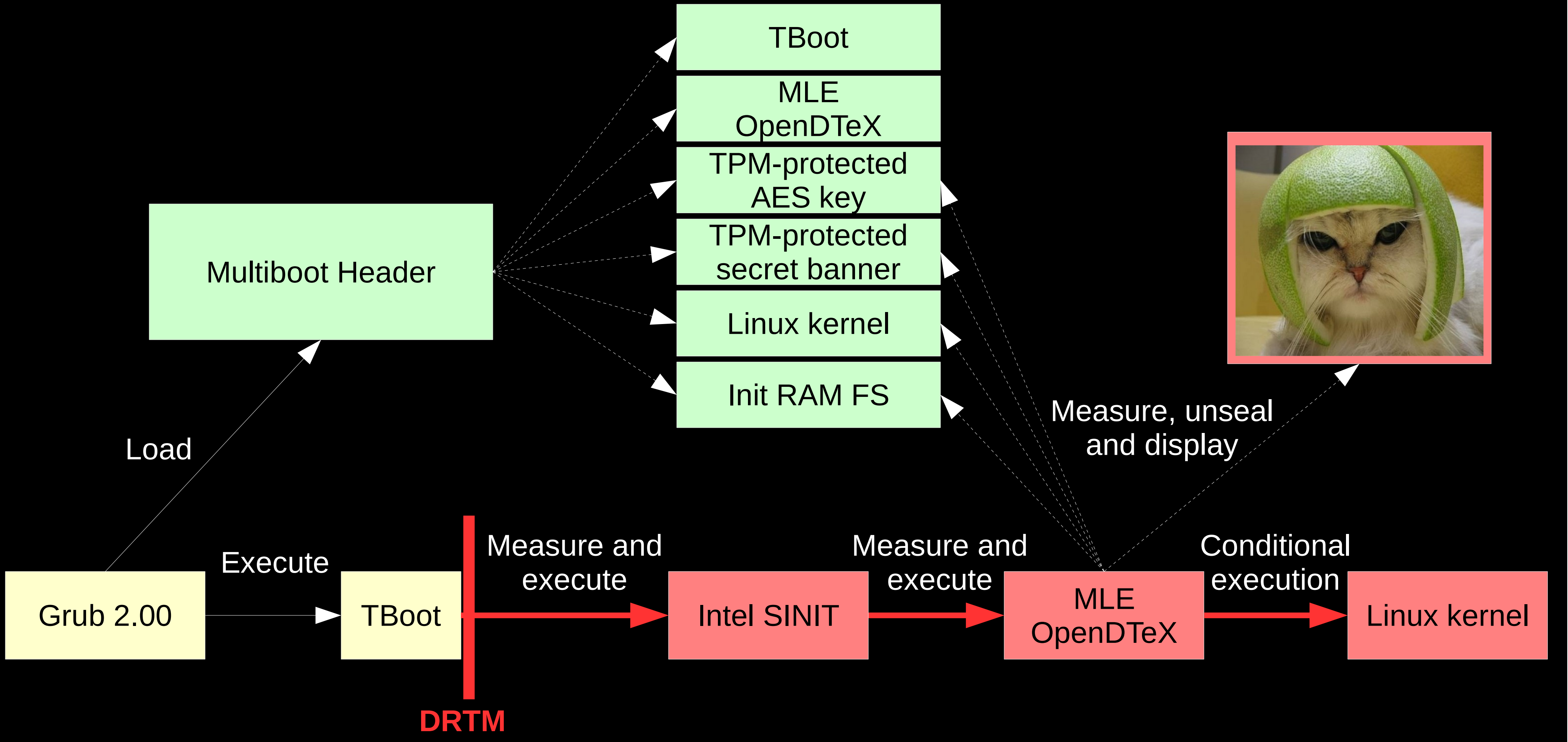
DRTM use case

- TPM
- Processor with hardware virtualization (Intel VT-x)
- Processor with SMX (Safer Mode Extensions)
- Chipset that supports Intel TXT and IOMMU (Intel VT-d) to allow DMA access control

OpenDTeX Secure Boot Developments

- Autonomous TPM 1.2 library
- Autonomous and minimal TSS library
- SRTM use case implementation
  - Extension of Grub 2.00 to support SRTM
- DRTM use case implementation
  - Extension of Intel TBoot with a dedicated DRTM MLE

OpenDTeX Secure Boot Architecture



Multiboot Header

TBoot

MLE
OpenDTeX

TPM-protected
AES key

TPM-protected
secret banner

Linux kernel

Init RAM FS

Load

Grub 2.00

Execute

TBoot

DRTM

Measure and
execute

Intel SINIT

Measure and
execute

MLE
OpenDTeX

Measure, unseal
and display

Conditional
execution

Linux kernel

Related work

Microsoft Bitlocker with TPM mode

- FDE protected laptop with TPM-bound key
- Limitation: doesn't address the fake UI problem, suffers from a large TCB and is exposed to DMA attacks

Anti-Evil-Maid PoC from J. Rutkowska

- TPM-sealed secret message
- Limitation: suffers from a large TCB and is exposed to DMA attacks due to SRTM

Intel TBoot

- Integrity measurement and verification through DRTM
- Limitation: does not provide proof to the user and no encryption

Conclusion

OpenDTeX provides Secure Boot for Linux

- With OS integrity verification...
- ...and attestation towards the user…
- ...along with file/kernel unsealing...
- ...either through SRTM or DRTM

Does not target every physical threats

- Hardware keylogger
- Hidden camera

Still work to do to provide strong physical security

Thanks for your attention!

OpenDTeX Secure Boot is released on

https://github.com/Amossys

@_sygus
@AMOSSYS