

Security Evolution on TV/OTT

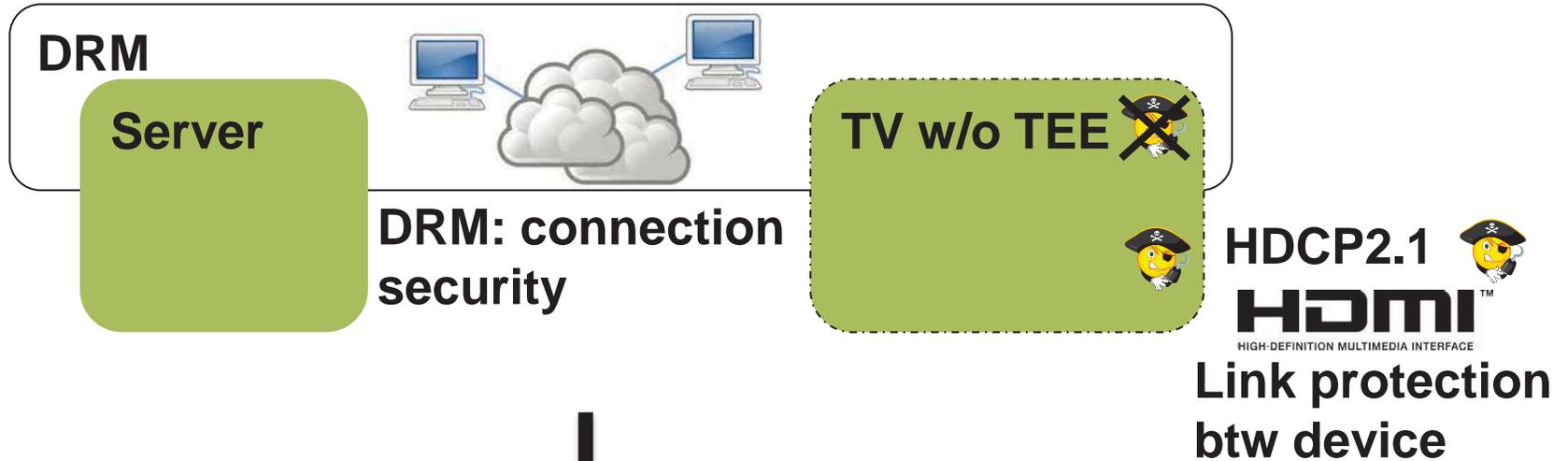


2015 Jun

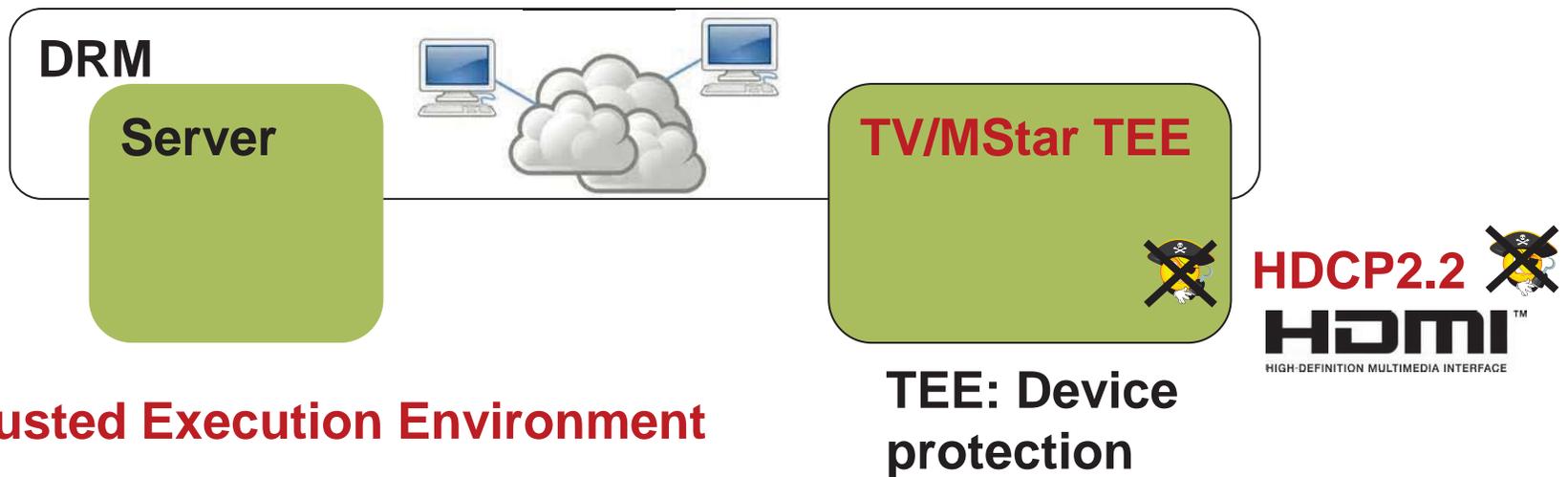
DRM vs Hardened DRM (TEE)



DRM

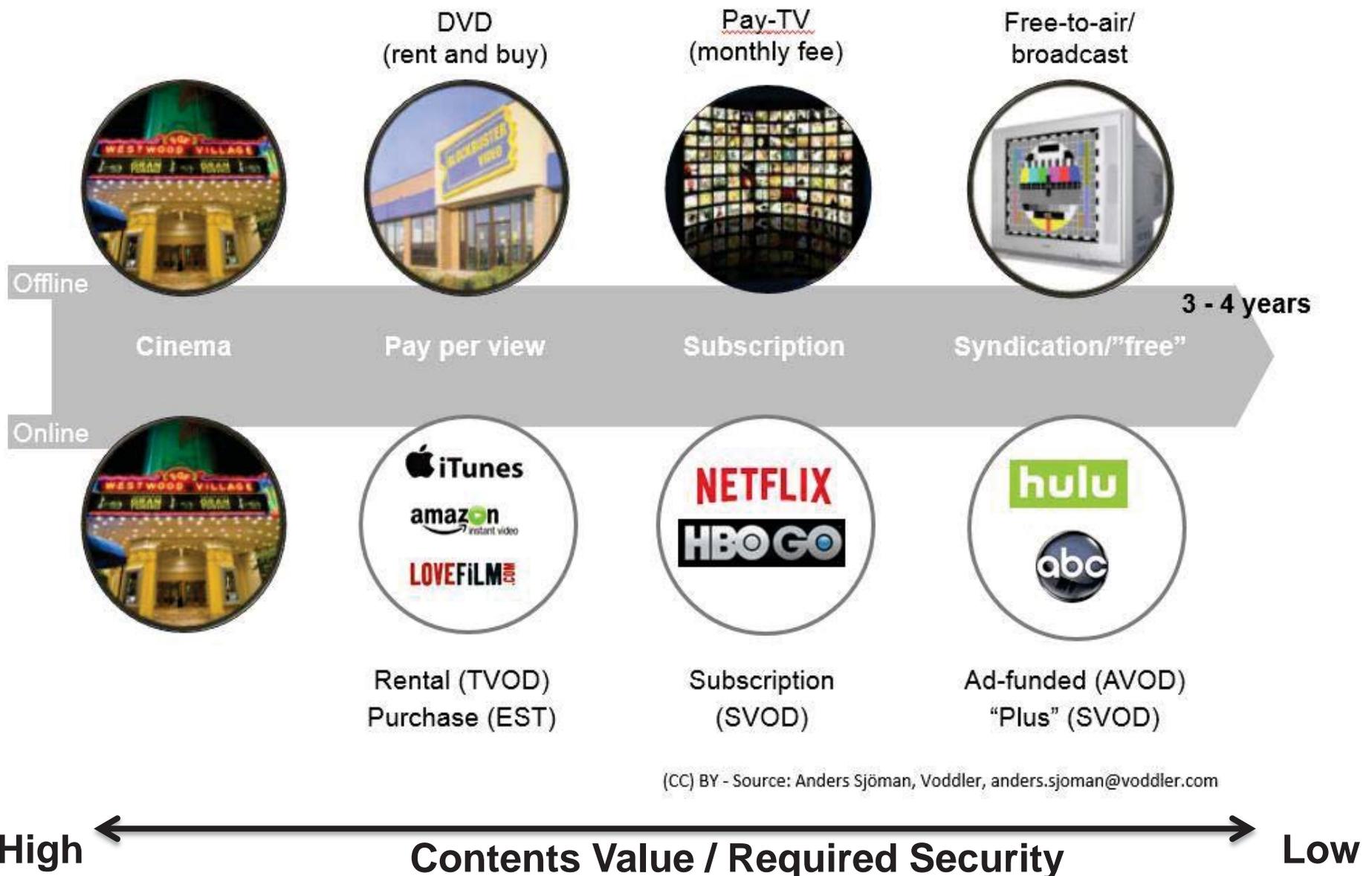


MStar TEE (Hardened DRM)



TEE – Trusted Execution Environment

High Security obtain Premium Contents – Easier/Cheaper



(CC) BY - Source: Anders Sjöman, Voddlar, anders.sjoman@voddlar.com

Security Required by Services



DRM

TEE



TEE
Others



TEE
Others

Movielab / Hollywood 4K

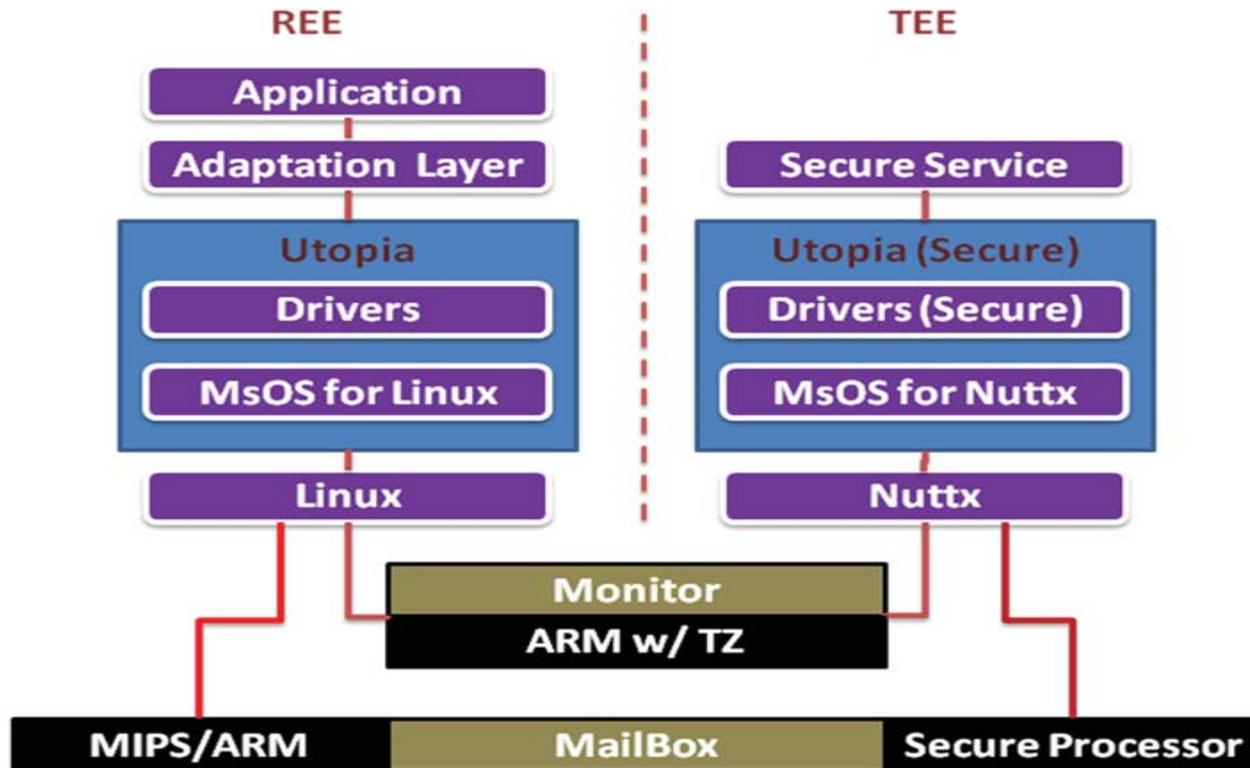
TEE
Others

What's TEE? What's Others?

MStar TEE (Global Platform)



MStar Security Platform



1. Decrypted Contents/ Key are processed in secure zone
2. Only Secure HW IP or Secure Processor can access secure zone
3. Non-security-related items are not in secure zone. ex. MM/ PVR
4. All info from normal zone are not trusted
5. Secure boot

Security – TEE



Based on HW

- AESDMA / HDCP2.2

Key Protection

- Managed by secure Processor/HW
- Stored in HW(OTP/ROM)
- Secure Store

Security Boot

- Boot Code in HW (OTP/ROM)
- Secure Update/Debug
- Unique Device ID

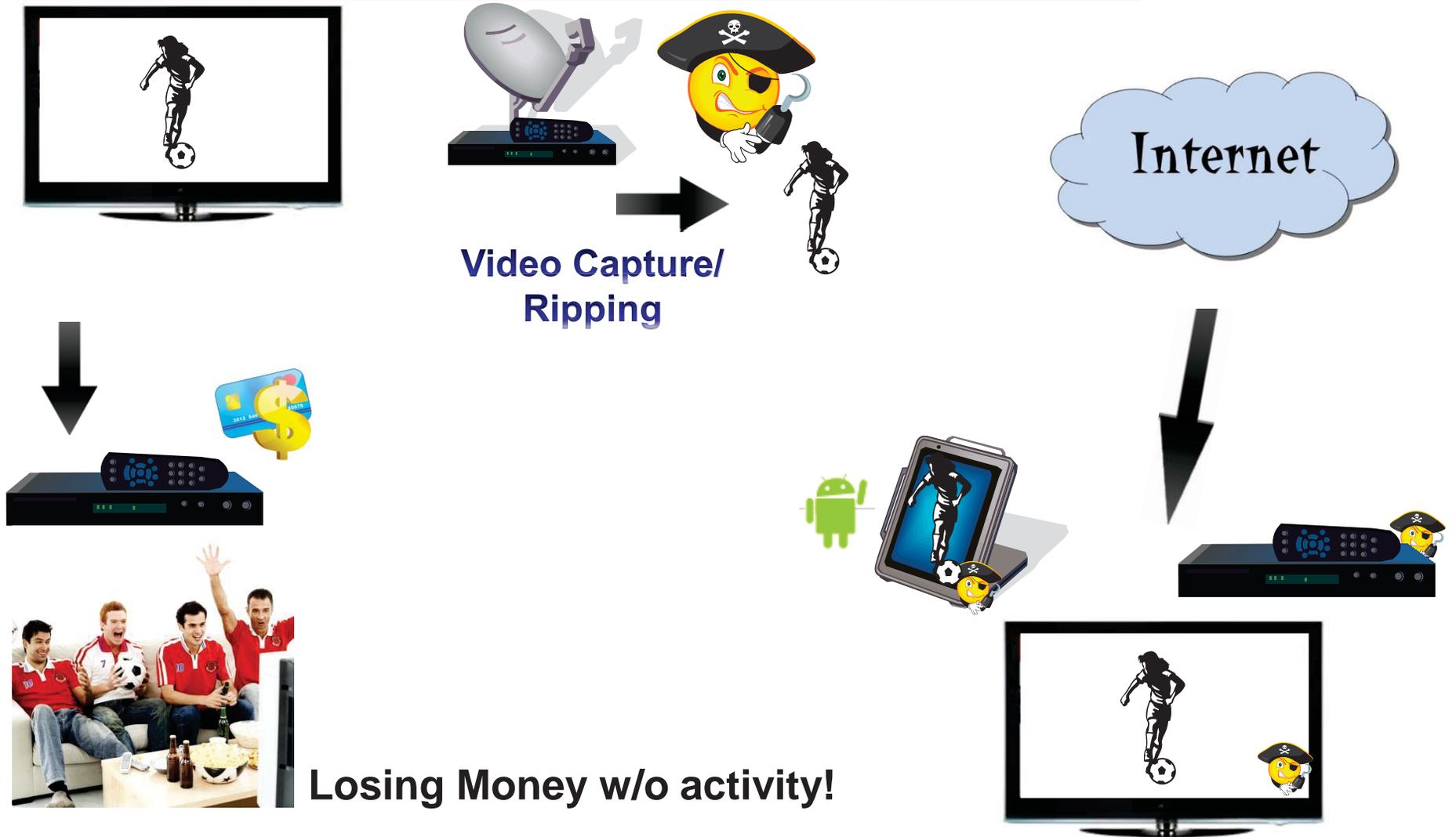
Secure Video Path

- Secure Range w/o memory burden
- DRAM Scramble w/o performance impact
- Protect Decompressed content

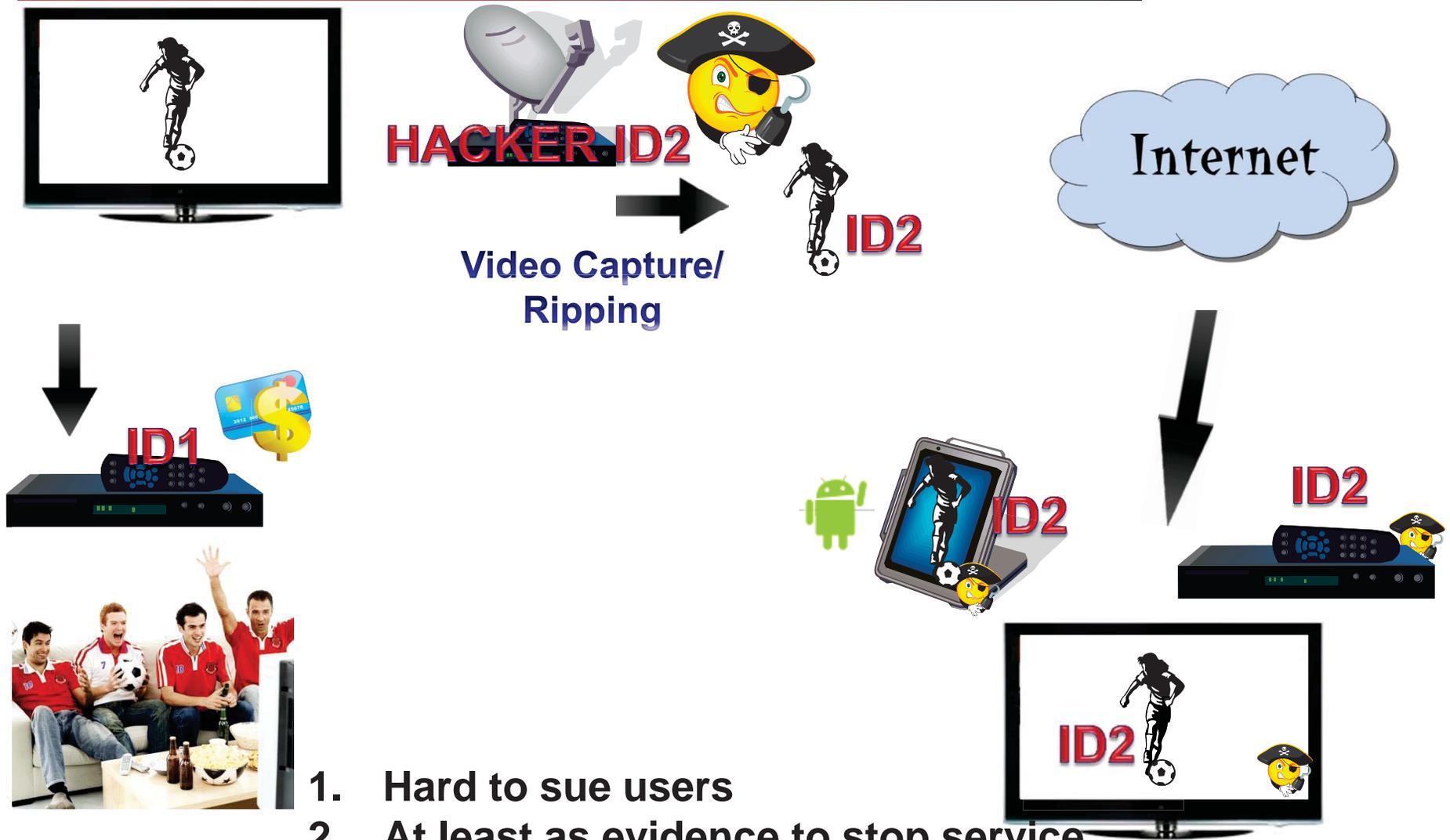
Concurrent

- Secure Processor Performance

Hacker Flow



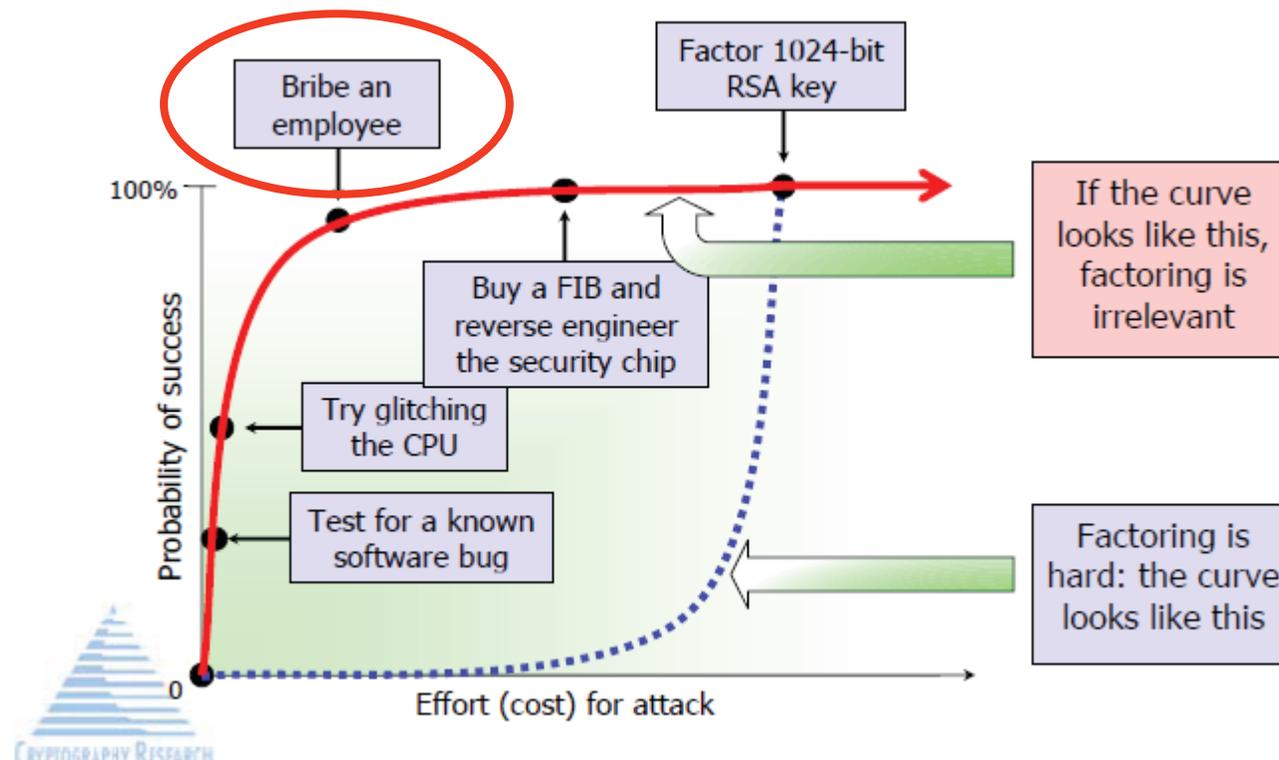
Hacker Flow with Watermark



1. Hard to sue users
2. At least as evidence to stop service
3. Easier to obtain premium content

3rd party HW ROT – Post Activation TV

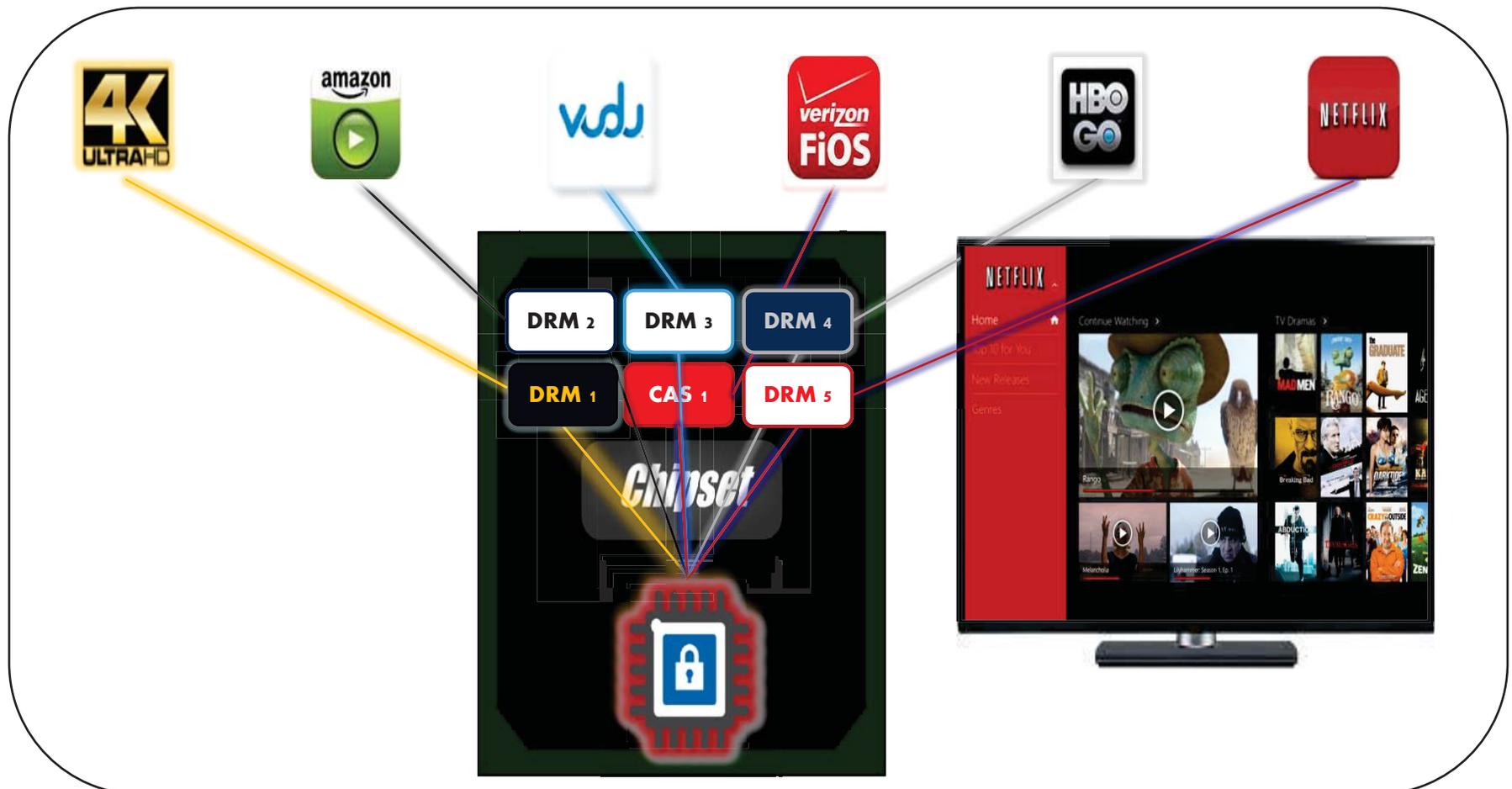
- 3rd party involvement to prevent human leakage – unique ID personalization, Key management
- 3rd party maintains good connections to Studios, easier to obtain certification
- Black box personalized for New Business Model – Post Activation TV



Business Model – Post Activation TV



1. New Service can be "On Shelf" after TV shipped out by downloading new app/SW
2. New Service/Application from MVPD/OTT/TV makers can be enabled for all accumulated TVs in the field
3. Support multiple CA/DRM depending each service providers' demand



Security – Beyond TEE



HW ROT (Root of Trust)

- Any 3rd HW ROT except MStar TEE

Forensic Watermark

- Can tapping be traced?

Watermark Detection

Playback

- Can limit function of pirate copy?

Anti Side Channel Attack

- Will Power/EMI...etc leak the key

TA Isolation

- How to separate different services' trusted application?

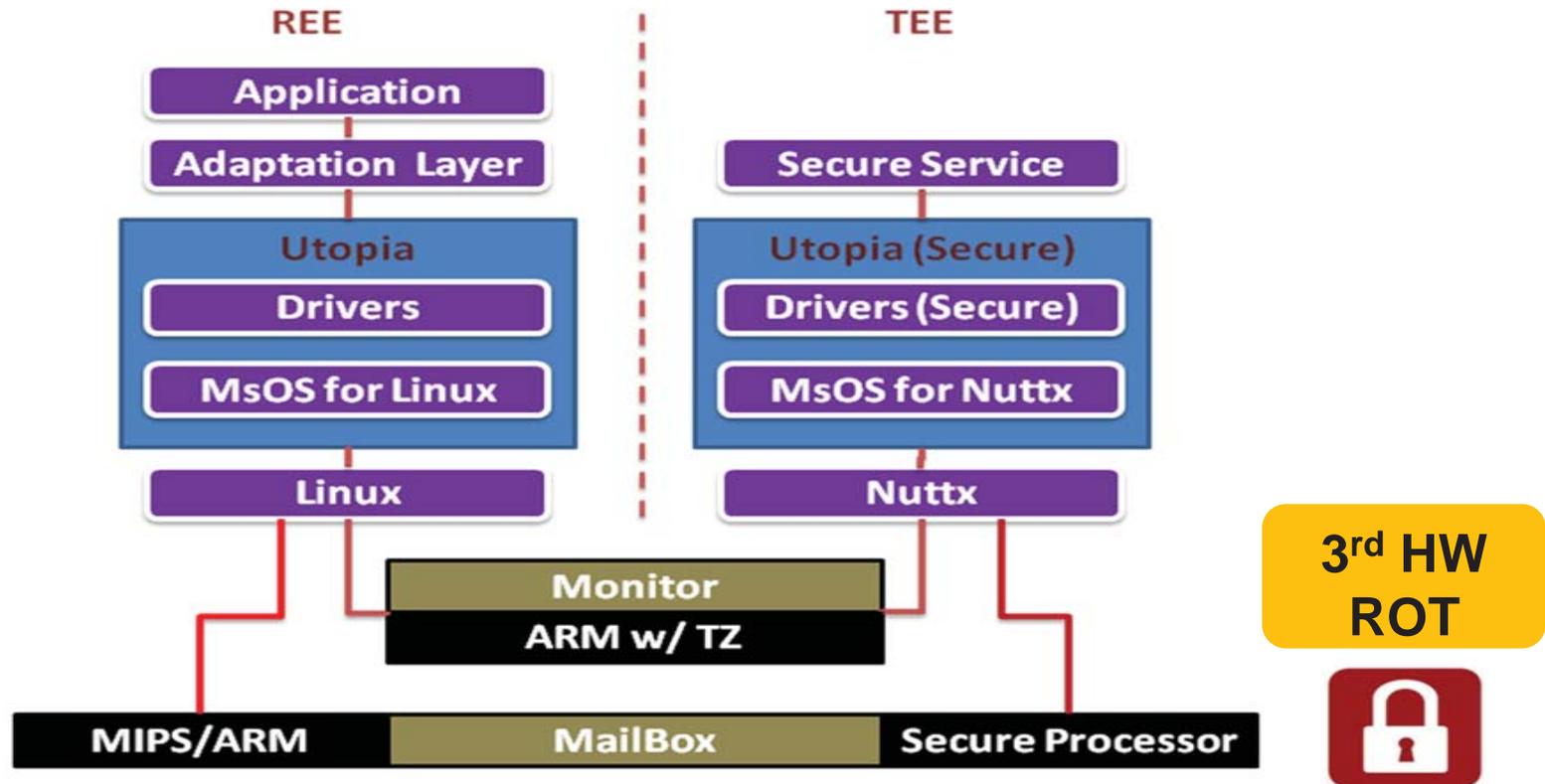
Certification

- Any 3rd party certification?

MStar TEE with 3rd party HW ROT



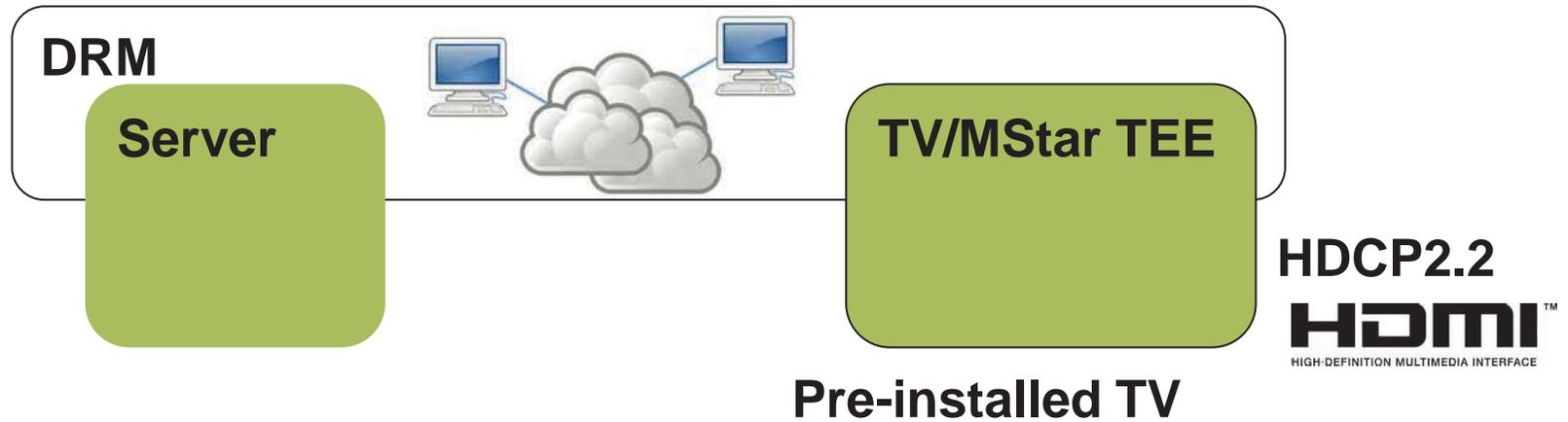
MStar Security Platform



1. TEE process based on 3rd party HW ROT
2. HW ROT based on Trusted vendors (CRI, Nagra)
3. Security reviewed by 3rd party

TEE vs TEE + HW ROT

MStar TEE



MStar TEE + HW ROT

