Vronicle: Verifiable Provenance for Videos from Mobile Devices

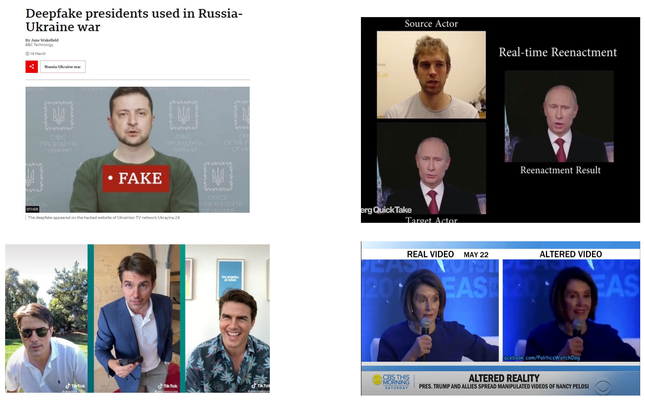
UCI University of California, Irvine

Yuxin (Myles) Liu, Yoshimichi Nakatsuka, Ardalan Amiri Sani, Gene Tsudik
University of California, Irvine

Microsoft

Sharad Agarwal
Microsoft

Fake/Manipulated Videos are Everywhere

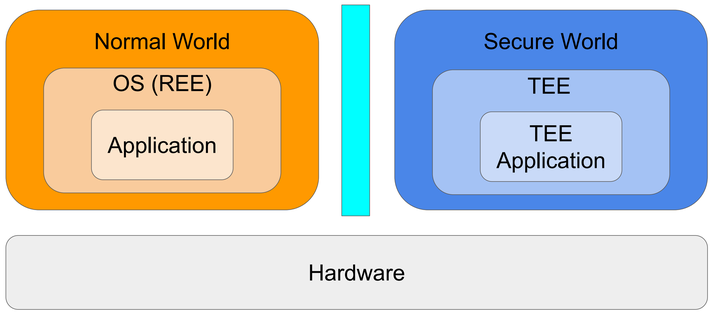


Instead of detection, let's do prevention

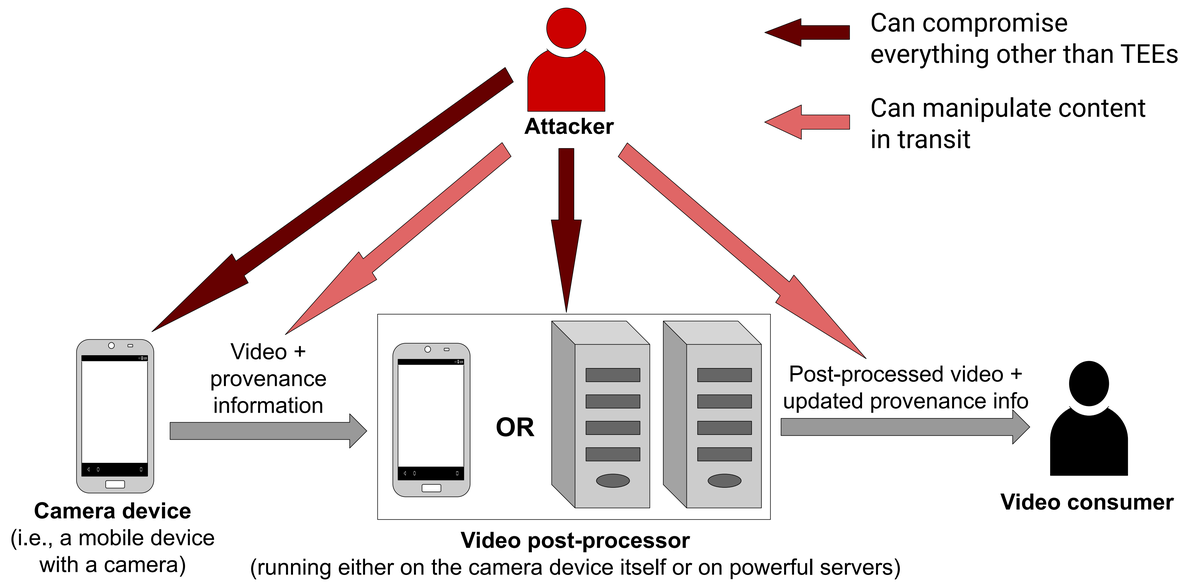
- Need verifiable fine-grained video provenance information that the consumer can use to gain high confidence that the video is authentic.
- Need decent performance of video post-processing.

TEE: Trusted Execution Environment

- A secure area in a processor that creates a completely isolated environment for a program to run.
- Examples: Intel SGX, AMD SEV, Arm TrustZone, …



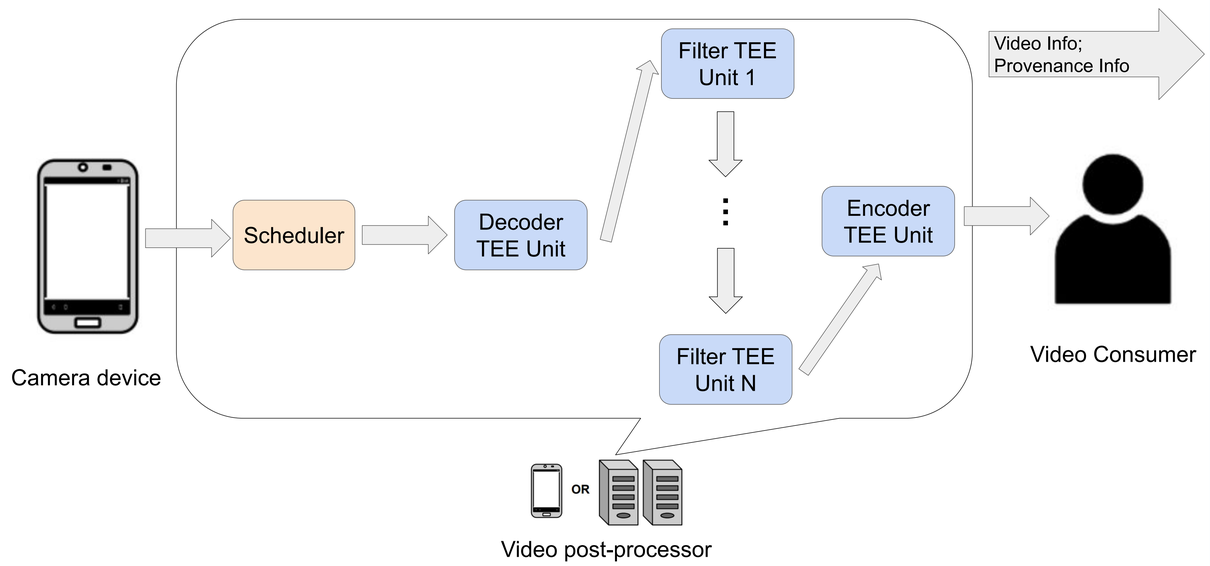
Our Vision



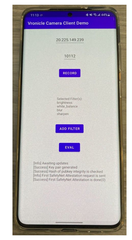
Key Point of Vronicle's post-processor

- *Fixed-function post-processing units*: help identifying each decoder/filter/encoder for verification.

Design of Vronicle's post-processor



Prototype



Camera device:
Galaxy S20 Plus

Azure Confidential Computing

Video post-processor:
Hickey 620 for Arm TrustZone;
Azure Confidential Computing VM for Intel SGX

Video consumer:
Ubuntu 20.04 Desktop