KASTEL - Institut für Informationssicherheit und Verlässlichkeit
Lehrstuhl Prof. Dr. J. Müller-Quade
https://crypto.kastel.kit.edu

Confidential Computing for Image Redaction

Bachelor's Thesis

Generative AI is widely used to create disinformation, both with respect to text and image contents. In order to defend against disinformation, the *Content Authenticity Initiative* has established the *C2PA* standard that allows to (cryptographically) attach „claims" of origin to e.g. photographs via digital signatures. Certain cameras, e.g. the Leica M11-P, natively supports the create of such claims. In particular, the Leica M11-P features a secure element that protects the signing key from malicious access. In such a setting, claims that a certain photography was taken with a certain camera are very plausible.

Unfortunately, the used digital signatures prevent the (transparent) redaction of images, which might be necessary to address e.g. privacy concerns of the photographer or photographed people. At the same time, simply re-signing the image after redaction breaks the link to the original signature. With this Bachelor's thesis, we want to build a technical solution that addresses this problem.

In more detail, we want to use trusted execution environments (TEEs), in particular the „cryptographic enclave" built by KASTEL, to perform image redaction. To this end, the TEE takes (a set of) images and verifies their associated C2PA claim, before it applies some user-provided operations on the image like adding Gaussian blur or scaling the image. The output consists of the processed images and new C2PA claims that documents both the original claims (e.g. that there was a valid signature by a Leica camera) and all transformations performed by the post-processor. By incorporating *remote attestation* of the computation, this new claim should be convincing to third parties.

The goal of this bachelor thesis is to develop a bootable and reproducible VM image that implements the described post-processing functionality. The design must also address security concerns, including the mitigation of side-channels.

Tasks & Requirements

- You must be a student in computer science or a related field of study and have experience with programming languages.
- You should be familiar with common signature schemes, virtualization, and networking protocols.
- In your work you should familiarize yourself with the C2PA standard.
- Compare different build systems to create reproducible Linux images (e.g. Buildroot, NixOS, Yocto Linux) based on their suitability and properties.
- Use a suitable build system to create a reproducible and bootable VM image that provides the post-processing functionality.
- Identify and protect critical assets, such as the signing key. Note that the implementation can be purely software-based, as we will adapt your contribution to our internal requirements.

Offer

- Opportunity to contribute to a research project that is planned for real-world deployment in the near future.
- Close supervision and guidance throughout the thesis.

Contact

In case of interest or for further information, please contact André Sperrle, andre.sperrle@kit.edu (Room 258, Building 50.34).