Leveraging the Uniqueness of Hardware Sensor Fingerprints for Spoofing-Resistant Mobile Device Authentication

Mobile device fingerprints are one answer to the “quest to replace passwords”.

- Multi-factor authentication
- Hardware-based fingerprints naturally reflect “something the user has”

Digital camera fingerprints are ideal candidates:
- Every camera has its own highly unique sensor noise fingerprint
- Stable and repeatable
- May augment existing authentication protocols based on visual codes

Caveat: fingerprint leakage in public images
- Sensor fingerprint estimate can be obtained from any image(s), by anyone
- Fingerprint spoofing made easy

Our Approach: Fragile Camera Fingerprints

Assumptions
- Alice’s smartphone can capture RAW images;
- Alice shares JPEG images in public only; i.e.,
- Eve is confined to estimate fingerprint from JPEGs

Implications: Exploit Asymmetries
- Camera verification based on fingerprint components that are fragile to JPEG compression
- Alice alone can provide correct device fingerprint

Building a Fragile Camera Fingerprint

\[ C = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \]

Cutoff parameter \( c \): High-frequency DCT coefficients are more susceptible to JPEG compression

Camera Verification and Spoofing

Building a fragile fingerprint

Challenges
- Fingerprint reuse across different services
- Storage/communication overhead

Non-ideal image capture conditions
- Fingerprint theft / revocation

Interested in meeting the PIs? Attach post-it note below!