Camera-based Mobile Device Authentication

PI: Matthias Kirchner, Binghamton University
http://www.ws.binghamton.edu/kirchner

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".[1,2]

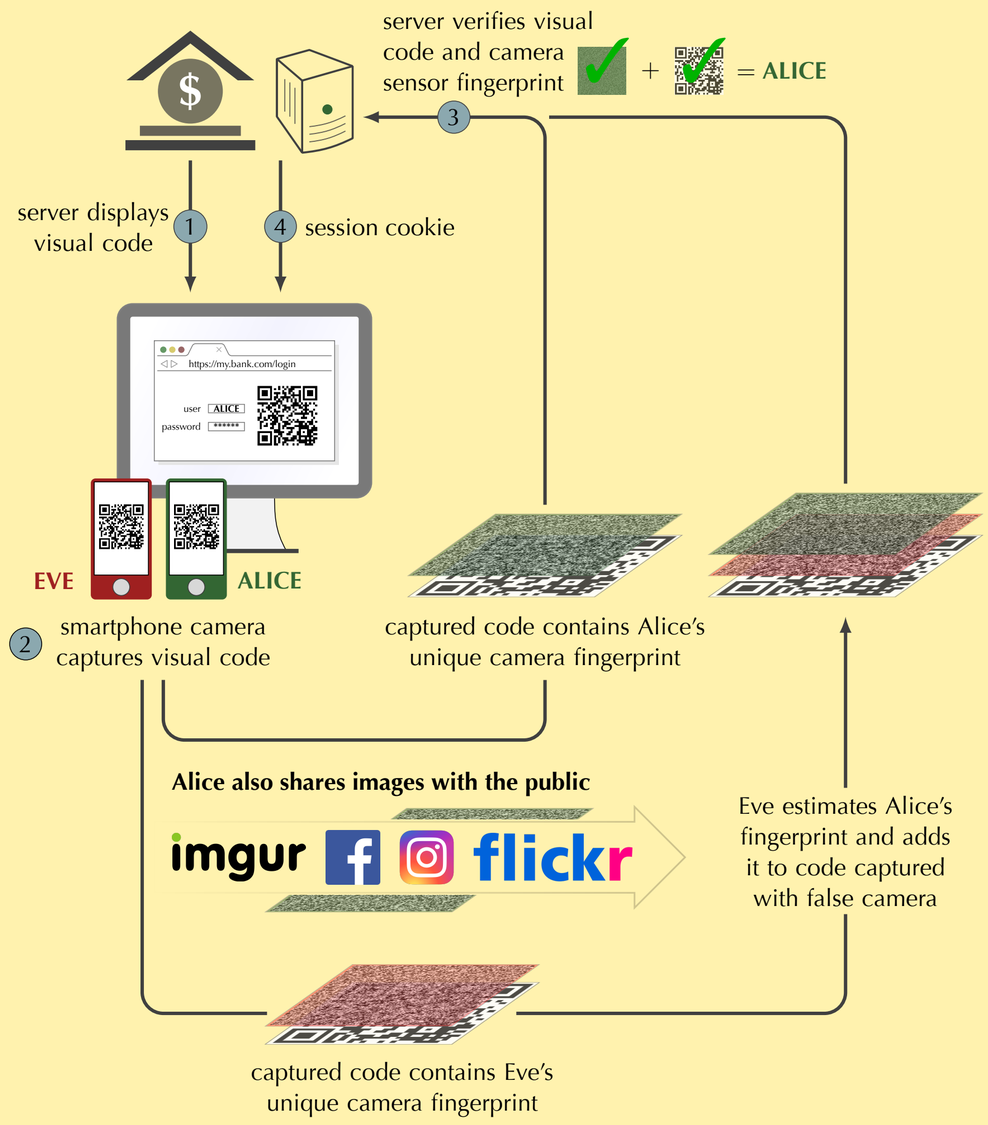
- Multi-factor authentication
- Hardware-based fingerprints naturally reflect "something the user has"

Digital camera fingerprints are ideal candidates:

- Every camera has its own highly unique sensor noise fingerprint[3]
- 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



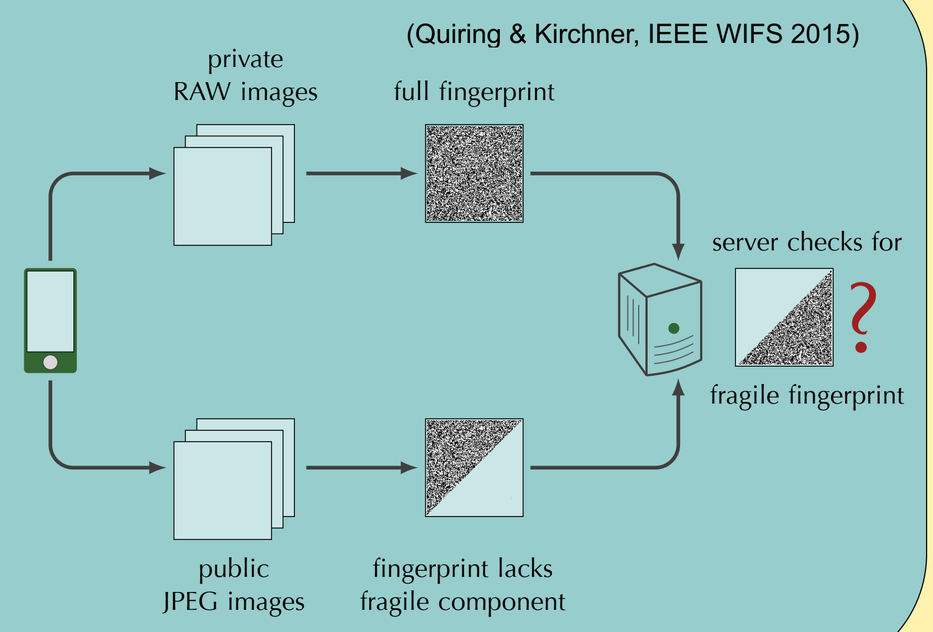
Our Approach: Fragile Camera Fingerprints

Assumptions

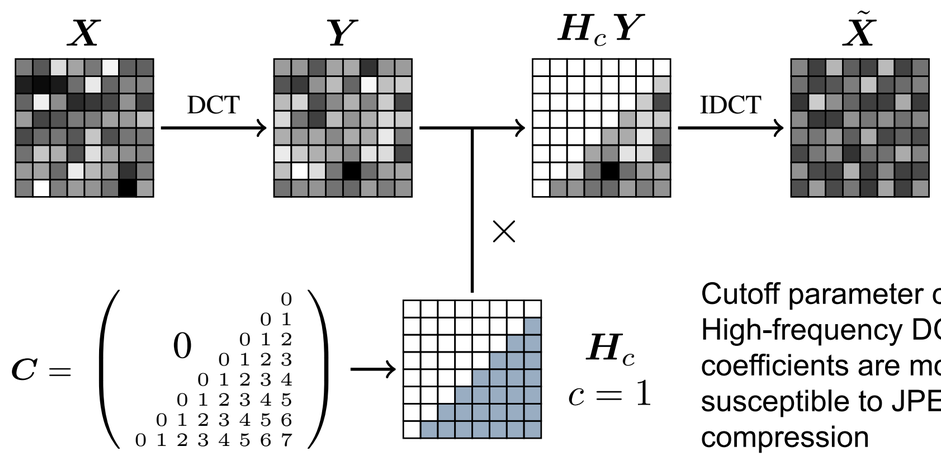
- Alice's smartphone can capture RAW images;
- Alice shares JPEG images in public only; i.e.,
- Eve is confined to estimate fingerprint from JPEGs

Implications: Exploit Asymmetries

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



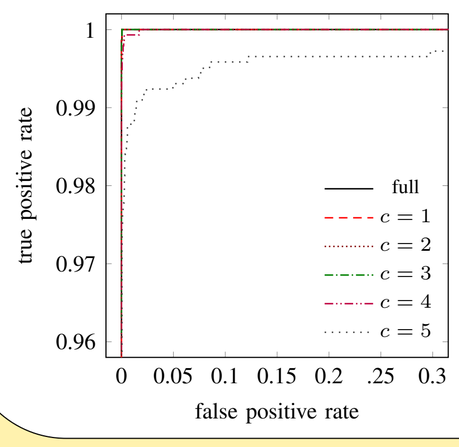
Building a Fragile Camera Fingerprint



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

Camera Verification and Spoofing

Verification for different cutoffs



Correlation spoofed vs. true fingerprint

JPEG	c = full	1	2	3	4	5
100	0.6128	0.6002	0.5565	0.4838	0.3828	0.2627
95	0.5291	0.3752	0.2645	0.1600	0.0800	0.0524
90	0.4381	0.1513	0.0762	0.0357	0.0169	0.0177
85	0.3758	0.0506	0.0154	0.0055	0.0023	0.0046
80	0.3347	0.0172	0.0009	-0.0014	-0.0008	0.0028
75	0.3035	0.0055	-0.0041	-0.0034	-0.0007	0.0016
70	0.2837	0.0015	-0.0053	-0.0042	-0.0015	0.0007
100	0.6414	0.6322	0.5924	0.5250	0.4302	0.3123
95	0.5704	0.4536	0.3464	0.2235	0.1173	0.0773
90	0.4798	0.2047	0.1087	0.0520	0.0243	0.0253
85	0.4167	0.0705	0.0231	0.0084	0.0028	0.0078
80	0.3756	0.0249	0.0024	-0.0019	-0.0013	0.0037
75	0.3445	0.0085	-0.0049	-0.0042	-0.0000	0.0027
70	0.3254	0.0036	-0.0063	-0.0059	-0.0008	0.0017

(spoofed fingerprint from 4600 images)

Challenges

- Fingerprint reuse across different services
- Storage/communication overhead
- Non-ideal image capture conditions
- Fingerprint theft / revocation

[1]Bonneau et al., IEEE S&P 2012; [2]Alaca & van Oorschot, ACSAC 2016; [3]Fridrich et al. 2005-16

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

The 3rd NSF Secure and Trustworthy Cyberspace Principal Investigator Meeting
January 9-11, 2017
Arlington, Virginia

National Science Foundation
WHERE DISCOVERIES BEGIN

BINGHAMTON UNIVERSITY
STATE UNIVERSITY OF NEW YORK