Security Impact of High Resolution Smartphone Cameras

Tobias Fiebig, Jan Krissler and Ronny Hänsch

Technische Universität Berlin
FG Security in Telecommunications and FG Computervision

WOOT 2014, San Diego, 19th of August 2014
This talk presents our work on "Security Impact of High Resolution Smartphone Cameras":

- By now nearly every smartphone has at least one, usually two high quality cameras.
This talk presents our work on "Security Impact of High Resolution Smartphone Cameras":

- "In Device" communication gets harder and harder with new multicompartment security measures.
This talk presents our work on "Security Impact of High Resolution Smartphone Cameras":

- Getting the camera permission with an evil app is apparently rather easy [Felt et al., 2011, Felt et al., 2012].
We demonstrate, that the front camera of modern smartphones can be used for visual keylogging. Without the need of physical proximity [Xu et al., 2013] and with higher precision than previous approaches [Simon and Anderson, 2013].

We evaluate the required border conditions and possible mitigation for this approach.

**Figure:** Approach of Xu et al. [Xu et al., 2013]
We demonstrate how and that an attacker can obtain high quality fingerprint images of a target, sufficient to utilize forgeries created from them on the most advanced sensors.
Figure: Based on data gathered from gsmarena.com end of February 2014.
Figure: Based on data gathered from gsmarena.com end of February 2014.
So... why does this happen?

- People do like the feature of having a camera with them... always.
So... why does this happen?

- Pictures taken should not be like... pixel-heaps.
And of course a front camera for serious video-conferencing!
And of course a front camera for serious video-conferencing!

- Ok, just kidding, more like for what the sales-droids call "generation selfie" - at least the high resolution ones, 8 Megapixel and up.
Attacker and Victim Model

- Attacker:
  - Somebody with a lot of resources...
  - With a lot of knowledge on computers...
  - Mainly attacking high-profile targets...
So, who might it be?
Interesting enough for our attacker.
About the victim...

- Interesting enough for our attacker.
- Probably using some fancy secure-phone.
About the victim...

- Interesting enough for our attacker.
- Probably using some fancy secure-phone.
- Probably somewhat well known... or something...
Uhmmmm... that's hard... any ideas...?
Yeah... might be her...
So, how do we do keylogging with the camera?

- Use reflections in the user's face.
So, how do we do keylogging with the camera?

- Use reflections in the user's face.
- Ideally sunglasses, worst case: eyes.
So, how do we do keylogging with the camera?

- Use reflections in the user's face.
- Ideally sunglasses, worst case: eyes.
- Used by Xu et al. for some really advanced shoulder surfing using e.g. camcorders while standing nearby [Xu et al., 2013].

**Figure**: Approach of Xu et al. [Xu et al., 2013]
Xu et al. had perfect reconstruction using the shadow of the moving (input) finger, if the display reflection in the recording had a size of around 10px.
Xu et al. had perfect reconstruction using the shadow of the moving (input) finger, if the display reflection in the recording had a size of around 10px.

Gave us a nice formula to calculate how big the reflection for a given camera and a given distance is:

\[
\text{Size}_{\text{Reflection}} = \left( \frac{\text{SensorResolution}}{\text{SensorSize}} \cdot \frac{\text{ObjectSize}}{\frac{\text{TargetDistance}}{\text{FocalLength}} - 1} \right) \cdot \frac{1}{\frac{2 \cdot \text{DistanceFromSurface}}{\text{CurvatureRadius}} + 1}
\]
Figure: Reflection-size in the user's eyes. Red line indicates border of perfect reconstruction. Everything above yields reconstructability.
What the user does.
What we see in the eye.
Zooming in.
A thumb!
Let's put on a keyboard.
Yep, that's a 3.
But what if our victims wears sunglasses?
Of course we prefer sunglasses like these...

Figure: Former Dr. jur. and German Secretary of Defense Karl-Theodor zu Guttenberg - currently neither.
**Figure:** Sunglasses can even make the keyboard of the device visible.
Provide amazing results!
Mitigation

- Viewport/Privacy filters:
- Randomized Keyboards:
- Gaze Based Passwords
- Biometric Authentication?
  - Let's see...
What issues may arise from the back camera?
What issues may arise from the back camera?

Biometry is kind of a big thing, especially in high security access controls...
So what about the other side...?

- What issues may arise from the back camera?

- Biometry is kind of a big thing, especially in high security access controls...

- ...and fingerprints are usually the poison of choice.
Think about this situation...

Figure: Red: Viewport of the camera.
Allowing us to do this:

(a) Captured Photo
(b) Extracted Binary Print
(c) Etched PCB negative
(d) Graphite applied
(e) Wood-glue applied
(f) Ready forgery
So, what can we do with this?

- Circumvent stationary access controls.
So, what can we do with this?

- Circumvent stationary access controls.
- Unlock somebodies iPhone.
So, what can we do with this?

- Circumvent stationary access controls.
- Unlock somebody's iPhone.
- Plant false prints somewhere
Circumvent stationary access controls.

Unlock somebodies iPhone.

Plant false prints somewhere
  At least last I heard "Officer, I have NO idea how my fingerprints got on that knife!" was not in the sum of things helping you in court...
So, what can we do with this?

- Circumvent stationary access controls.
- Unlock somebodies iPhone.
- Plant false prints somewhere
  - At least last I heard "Officer, I have NO idea how my fingerprints got on that knife!" was not in the sum of things helping you in court...
- Track users across devices. (Ok, we do not need the forgeries for that... )
Front-cameras in smartphones make rather good keyloggers.
Front-cameras in smartphones make rather good keyloggers.

Back-cameras are rather useful at extracting biometric features.
Front-cameras in smartphones make rather good keyloggers.

Back-cameras are rather useful at extracting biometric features.

Mitigation is hard.
Figure: Seriously... having those hardwareshutters again would be nice
