PIN Skimming: Exploiting the Ambient-Light Sensor in Mobile Devices

Raphael Spreitzer
IAIK, Graz University of Technology, Austria

SPSM @ ACM CCS 2014, Scottsdale, Arizona, 7th November 2014

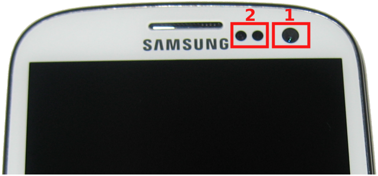
Outline

- Introduction & motivation
- Ambient-light sensor
- Attack scenario
- Evaluation of results
- Mitigation techniques
- Conclusion

Introduction & Motivation

- Wide-spread usage of mobile devices
  - Entertainment applications
  - Business applications (*e.g.*, banking)
- Protection of private information
- Features/sensors that can be exploited
  - Camera, sound, motion sensors, ...
  - Less obvious: ambient-light sensor

Ambient-Light Sensor

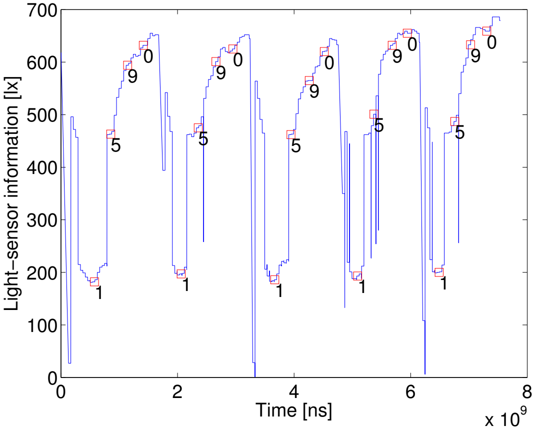


1) Front camera

2) Ambient-light sensor

- Intensity of surrounding illumination
- Adapt screen brightness
- Android Sensor API ($\sim$750 Hz)

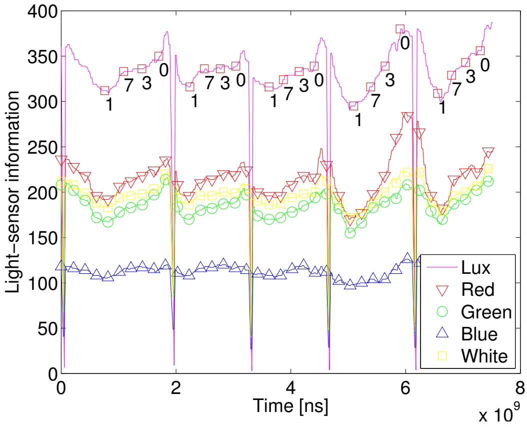
Information Leakage



- Prompt user to enter a random 4-digit PIN

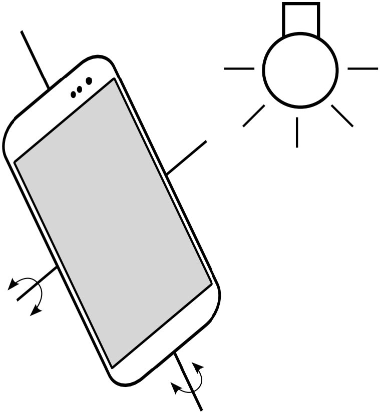
RGBW Sensor

- No API support → read virtual filesystem directly



Observation

- Tilts and turns during smartphone operation



Assumptions

- User is holding the device in his hands
- PIN is entered on a keypad rather than a QWERTY keyboard
- Light sensor faces sufficiently large variance of ambient light
- Training data and test data is collected in the same environment

Attack Scenario

Training phase

- A game to collect the training data (labeled data)
- Learn a specific set of PINs

Attack phase

- Trick user into starting the application to be attacked
- Collect sensor values in the background
- Infer PIN by means of machine learning

Security implications

- Samsung KNOX [SA13]
- BYOD
- Attack “business” world from “private” world

Setup

Unconstrained environments (rooms)

- Uniformly lit via tube lights
- Standard ceiling lamp
- Window as the only light source
  - Even considered different daytimes
  - Diffuse light conditions

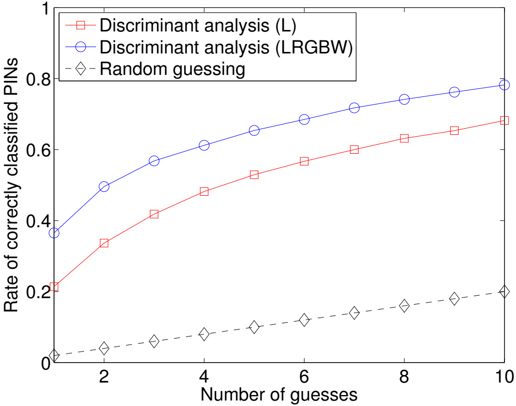
Users were asked not to walk around

- Compliant with our attack scenario

We did not insist on a specific input method

Correctly Classified PINs after Guessing

- Based on a set of 50 learned PINs



Comparison with Related Work

Attacks targeting a set of 50 PINs

	[ASBS12]	[SA13]	Ours
Sensor	Accelerometer	Camera	Ambient-light sensor
Permissions	Internet	Camera, Internet	Internet
Input method	No constraints	Thumb of holding hand	No constraints
Accuracy	43% within 5 guesses	50% within 5 guesses	65% within 5 guesses

Our attack works at least as good as related attacks

Countermeasures

UI and API modifications

- Disable sensors during “sensitive” input? [ASBS12]
- Varying keyboard layout [OHD$^+$12]
- Restrict access to OS

Permission model & application analysis

- OS developers need to deal with this problem
- Install-time warning [FEF$^+$12, FHE$^+$12]
- Scan apps during the installation

$\Rightarrow$ Raise user awareness

Conclusion

Summary

- Ambient-light sensor leaks sensitive information
- No permission required
- Developed a proof-of-concept application

Future work

- Detailed comparison of sensor-based attacks
- Combination of sensors

PIN Skimming: Exploiting the Ambient-Light Sensor in Mobile Devices

Raphael Spreitzer
IAIK, Graz University of Technology, Austria

SPSM @ ACM CCS 2014, Scottsdale, Arizona, 7th November 2014

Bibliography I

[ASBS12] Adam J. Aviv, Benjamin Sapp, Matt Blaze, and Jonathan M. Smith.
Practicality of Accelerometer Side Channels on Smartphones.
In *Annual Computer Security Applications Conference (ACSAC)*, pages 41–50, 2012.

[FEF+12] Adrienne Porter Felt, Serge Egelman, Matthew Finifter, Devdatta Akhawe, and David Wagner.
How to Ask for Permission.
In *USENIX Conference on Hot Topics in Security (HotSec)*, 2012.

[FHE+12] Adrienne Porter Felt, Elizabeth Ha, Serge Egelman, Ariel Haney, Erika Chin, and David Wagner.
Android Permissions: User Attention, Comprehension, and Behavior.
In *Symposium On Usable Privacy and Security (SOUPS)*, page 3, 2012.

[OHD+12] Emmanuel Owusu, Jun Han, Sauvik Das, Adrian Perrig, and Joy Zhang.
ACCessory: Password Inference using Accelerometers on Smartphones.
In *Mobile Computing Systems and Applications (HotMobile)*, page 9, 2012.

Bibliography II

[SA13] Laurent Simon and Ross Anderson.

PIN Skimmer: Inferring PINs Through The Camera and Microphone.

In *ACM Workshop on Security and Privacy in Smartphones & Mobile Devices (SPSM)*, pages 67–78, 2013.