PlaceRaider

Virtual Theft in Physical Spaces with Smartphones

Robert Templeman
Naval Surface Warfare Center, Crane Division
Indiana University Bloomington

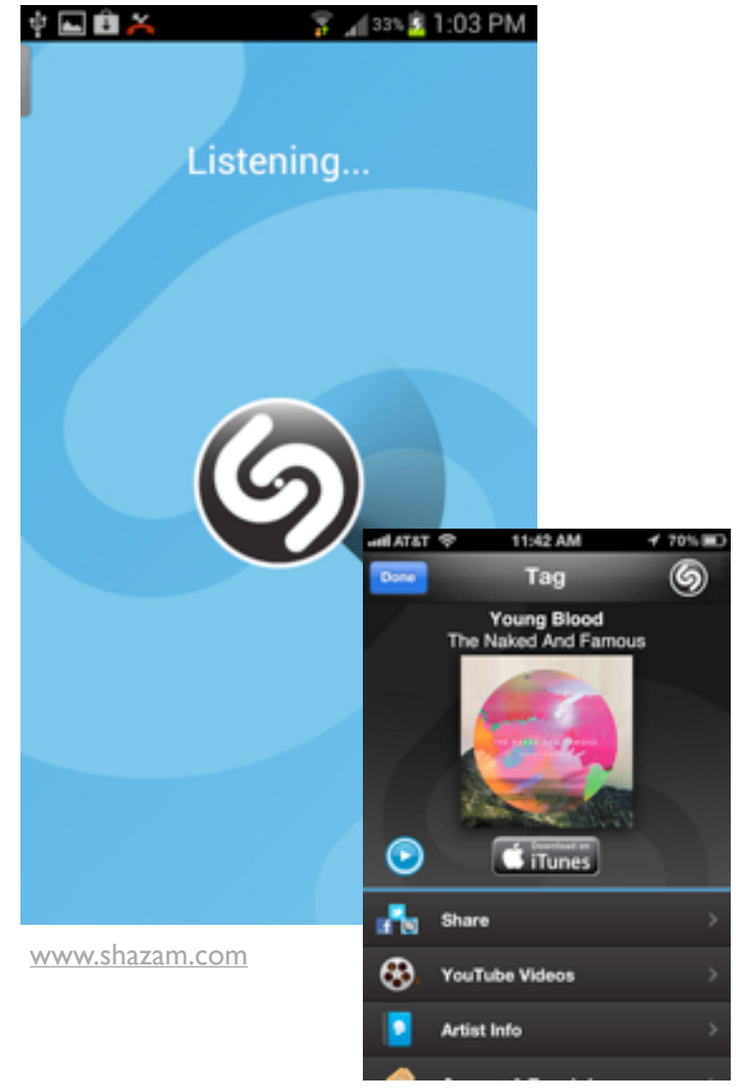
Zahid Rahman, David Crandall, Apu Kapadia
Indiana University Bloomington

NAVSEA WARFARE CENTERS CRANE

INDIANA UNIVERSITY
SCHOOL OF INFORMATICS AND COMPUTING
Center for Security Informatics
Bloomington

Today's smartphones are highly capable sensing platforms

http://www.google.com/mobile/skymap/



www.shazam.com

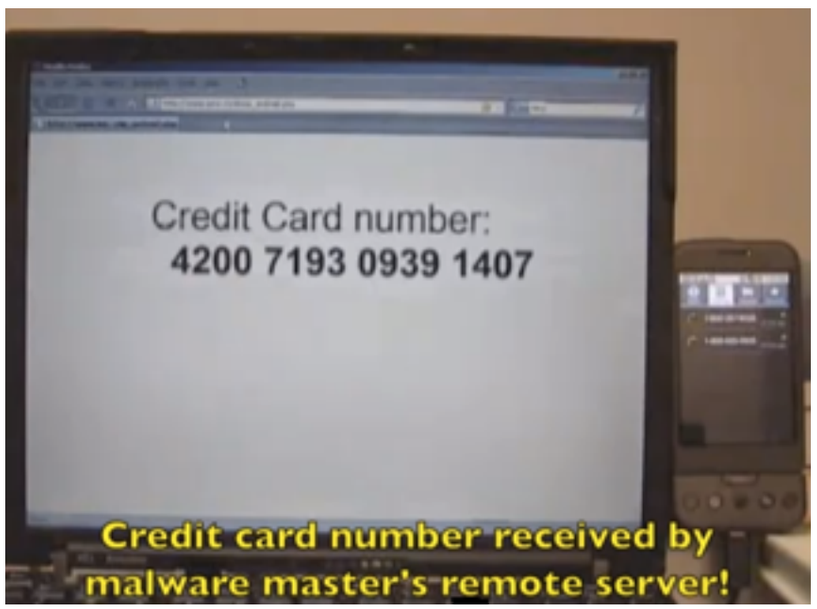
www.kronospark.com

NAVSEA WARFARE CENTERS CRANE

INDIANA UNIVERSITY

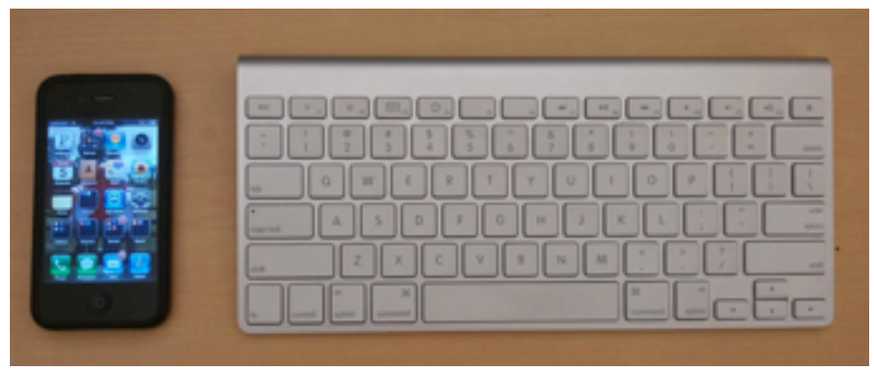
These sensors allow for a new generation of **sensory malware**

Hearing credit card numbers



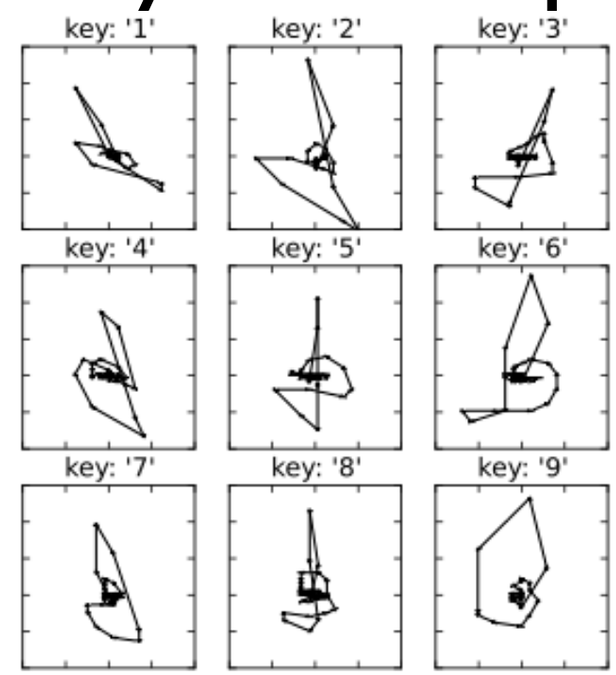
Soundcomber
Schlegel et al.
NDSS '11

Feeling keystrokes with accelerometer



(sp)iPhone
Marquardt et al.
CCS '11

Feeling Soft-keyboard taps



TouchLogger
Cai and Chen
HotSec '11

NAVSEA WARFARE CENTERS CRANE

INDIANA UNIVERSITY

We explore sensory malware with the **sense of sight**

(beyond taking compromising photos)

Virtual Theft

Performing remote reconnaissance and *targeted theft* using the victim's camera

Attacker **loses control** of the camera
Faced with a **data deluge**
Cannot make sense of the environment

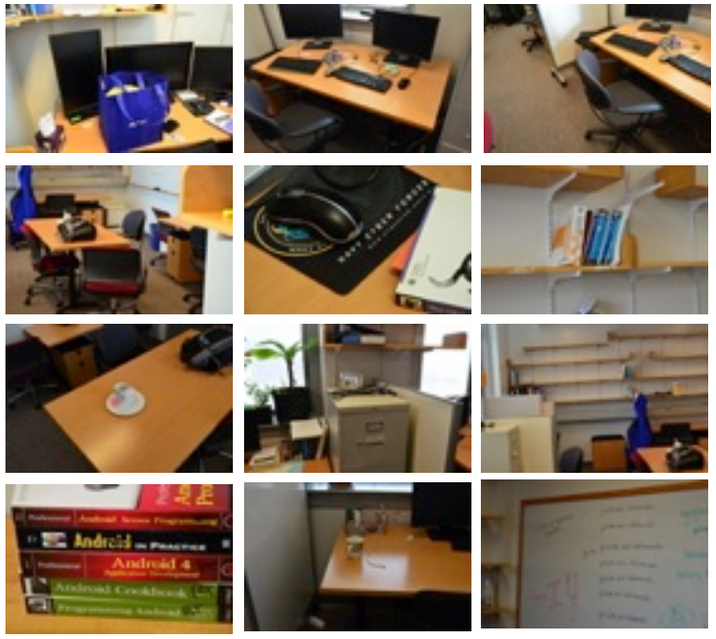
*Can the attacker reconstruct a **3D model** of the victim's space for structured navigation?*

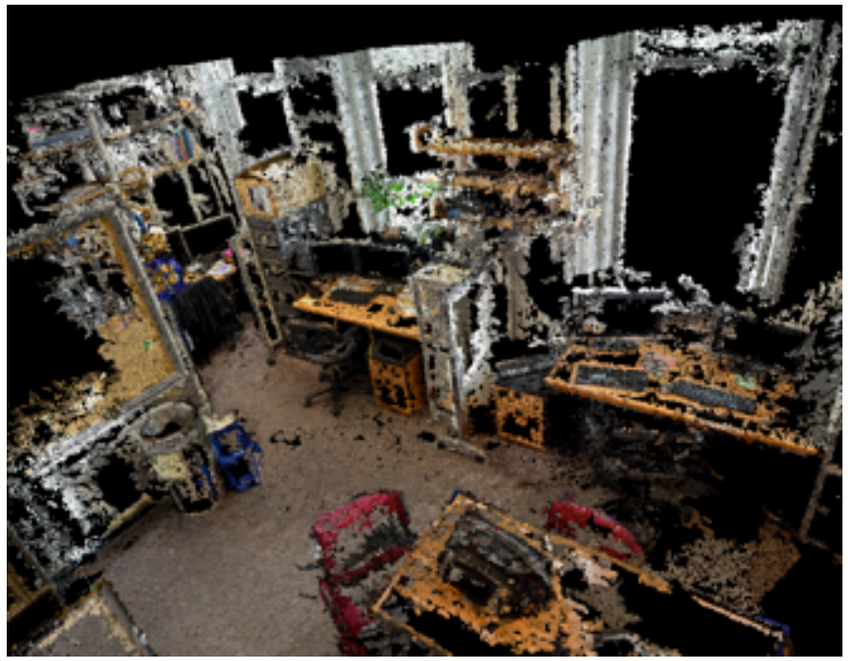
Building 3D models from images

Photo Tourism, Snavely et al. 2006
Building Rome in a Day, Agarwal et al. 2009
Building Rome on a Cloudless Day, Frahm et al. 2010
Accurate, Dense, and Robust Multiview Stereopsis, Furukawa et al. 2010
SfM with MRFs, Crandall et al. 2012

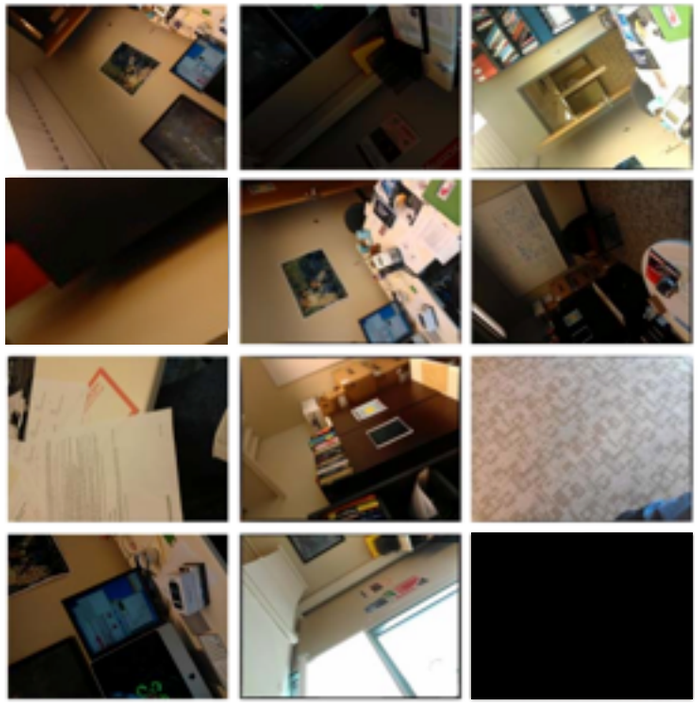
Can we generate good 3D models from surreptitiously taken photos?

Deliberate Photos





Opportunistic Photos



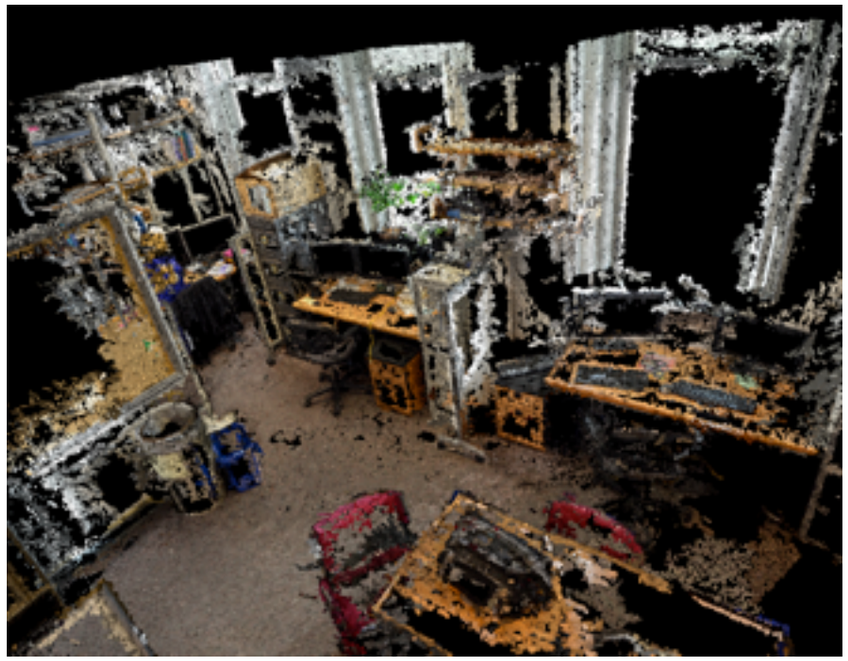
?

NAVSEA WARFARE CENTERS CRANE

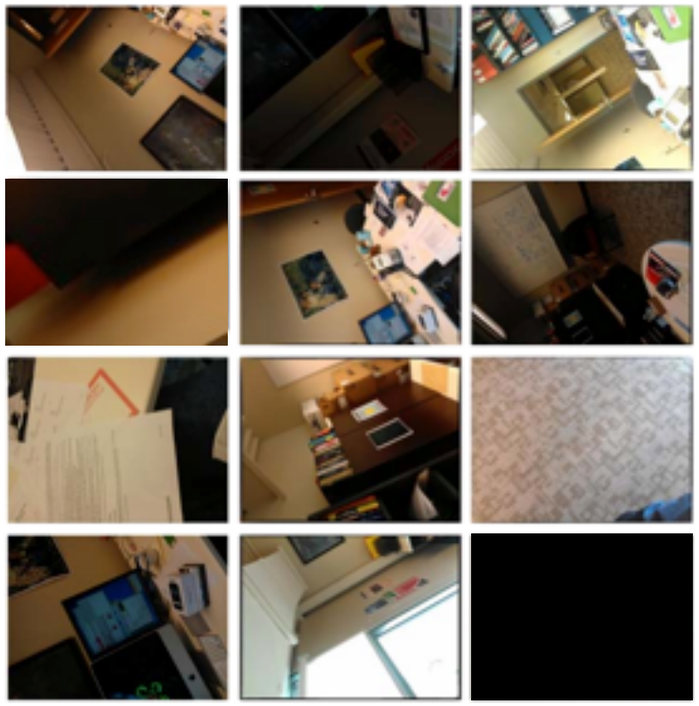
INDIANA UNIVERSITY

Can we generate good 3D models from surreptitiously taken photos?

Deliberate Photos

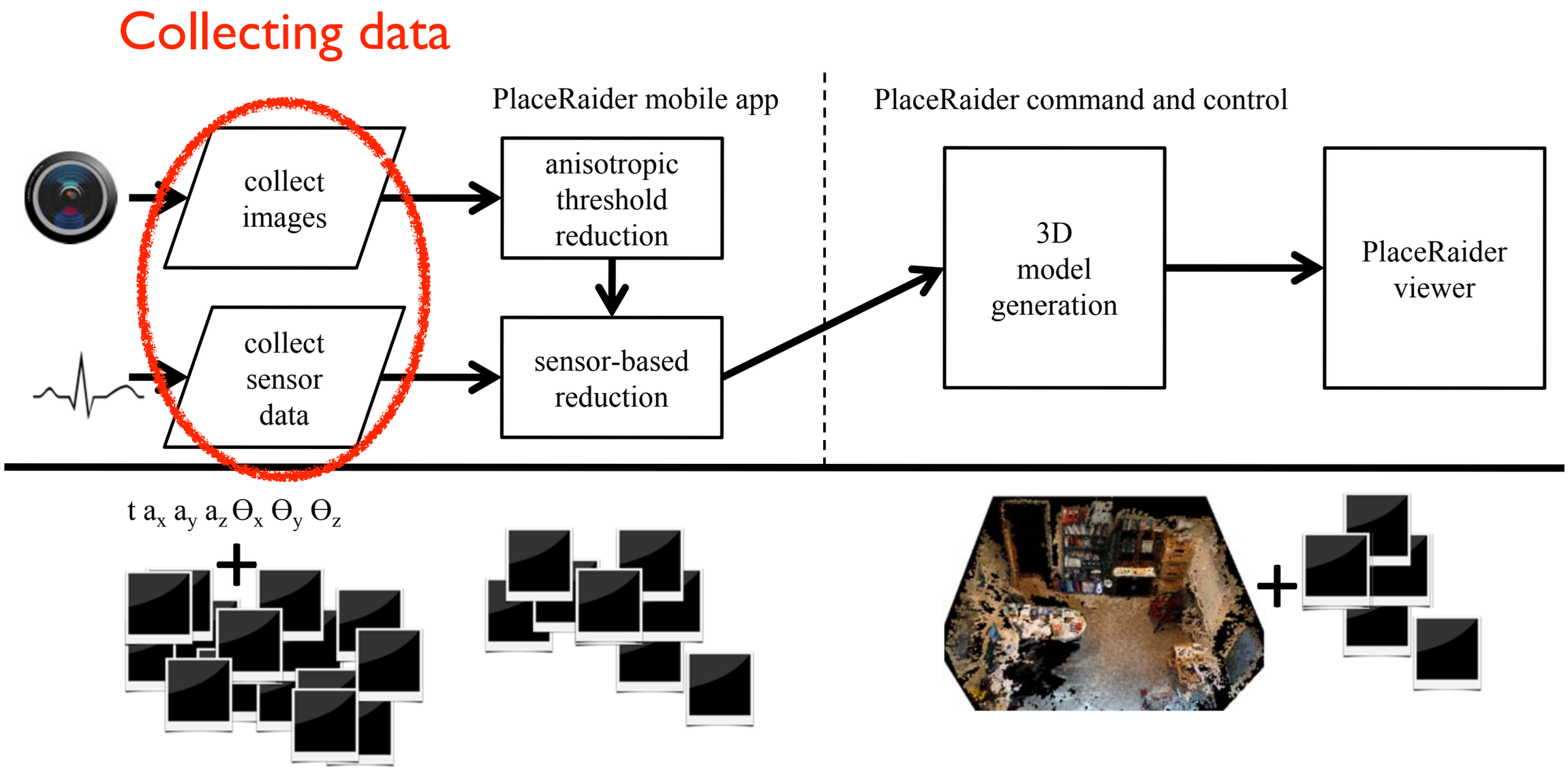


Opportunistic Photos

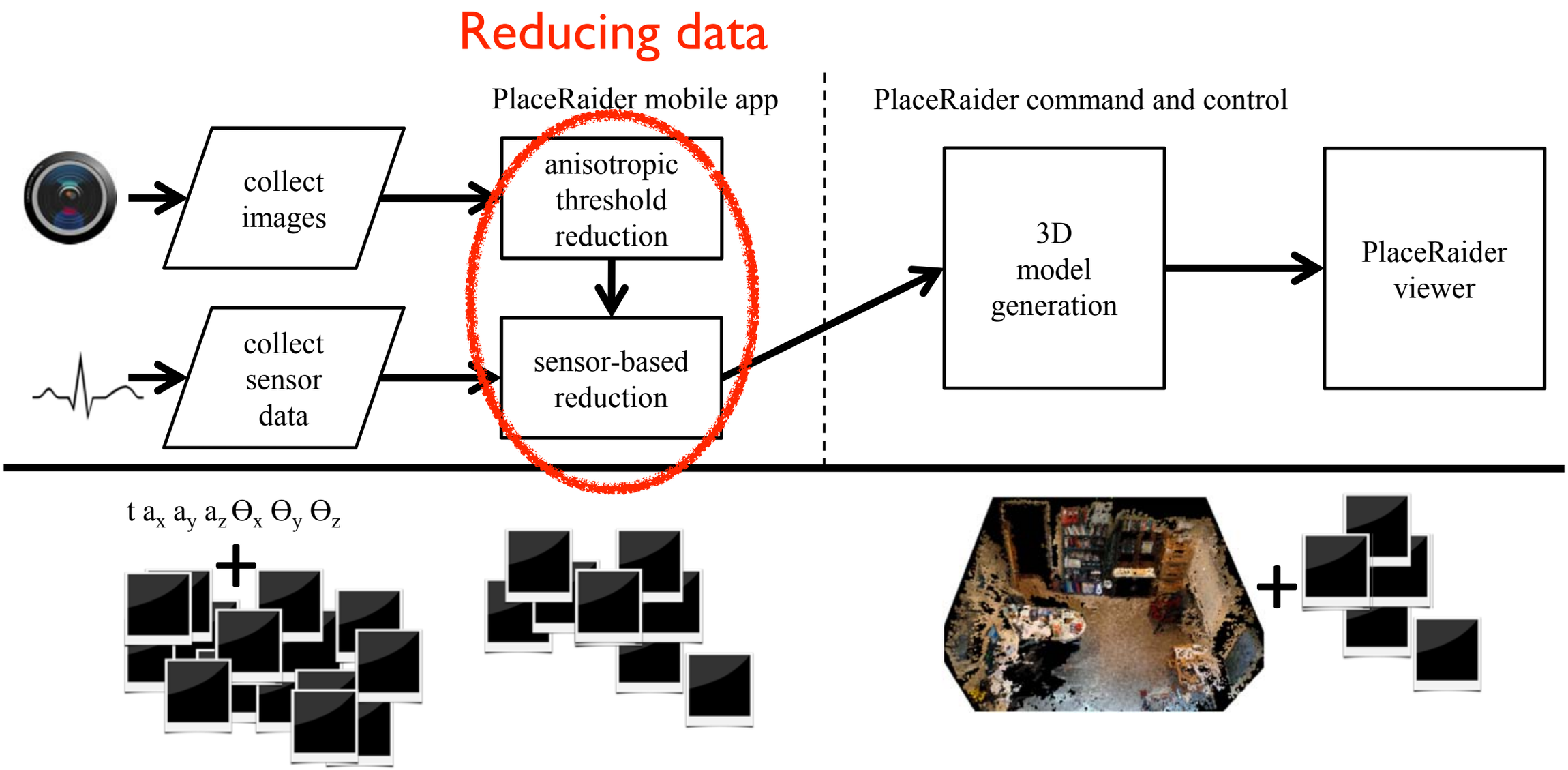


NAVSEA WARFARE CENTERS CRANE

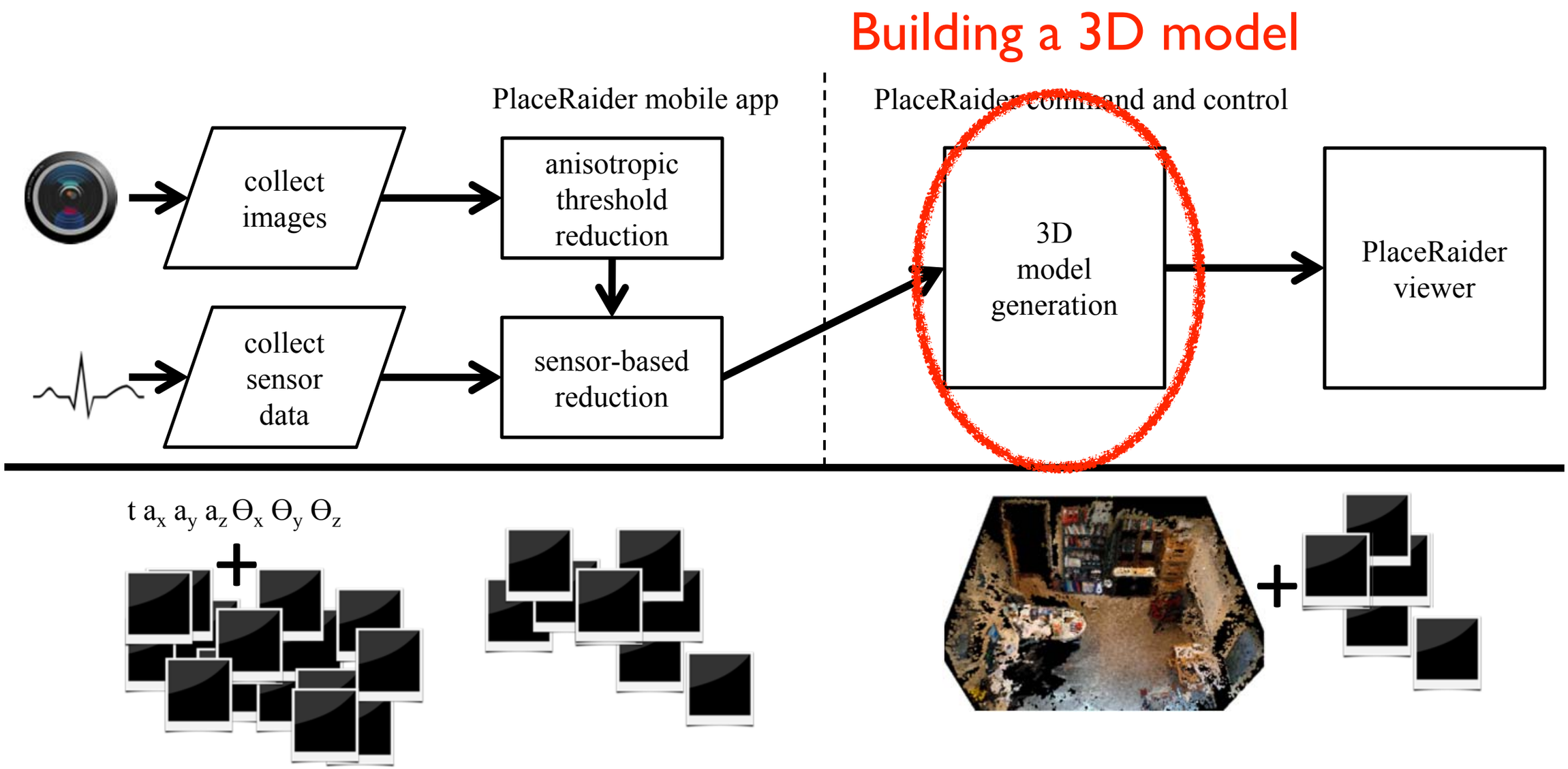
PlaceRaider Architecture



PlaceRaider Architecture

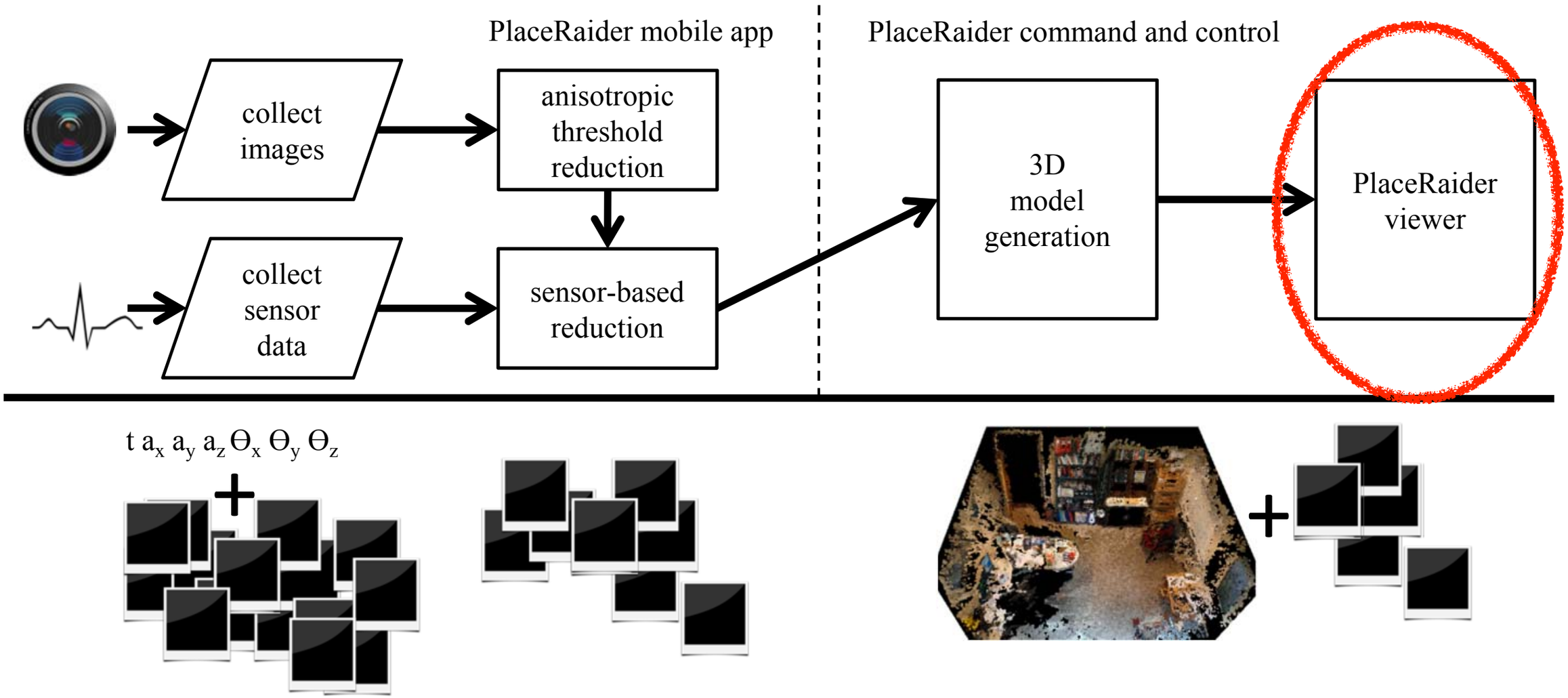


PlaceRaider Architecture

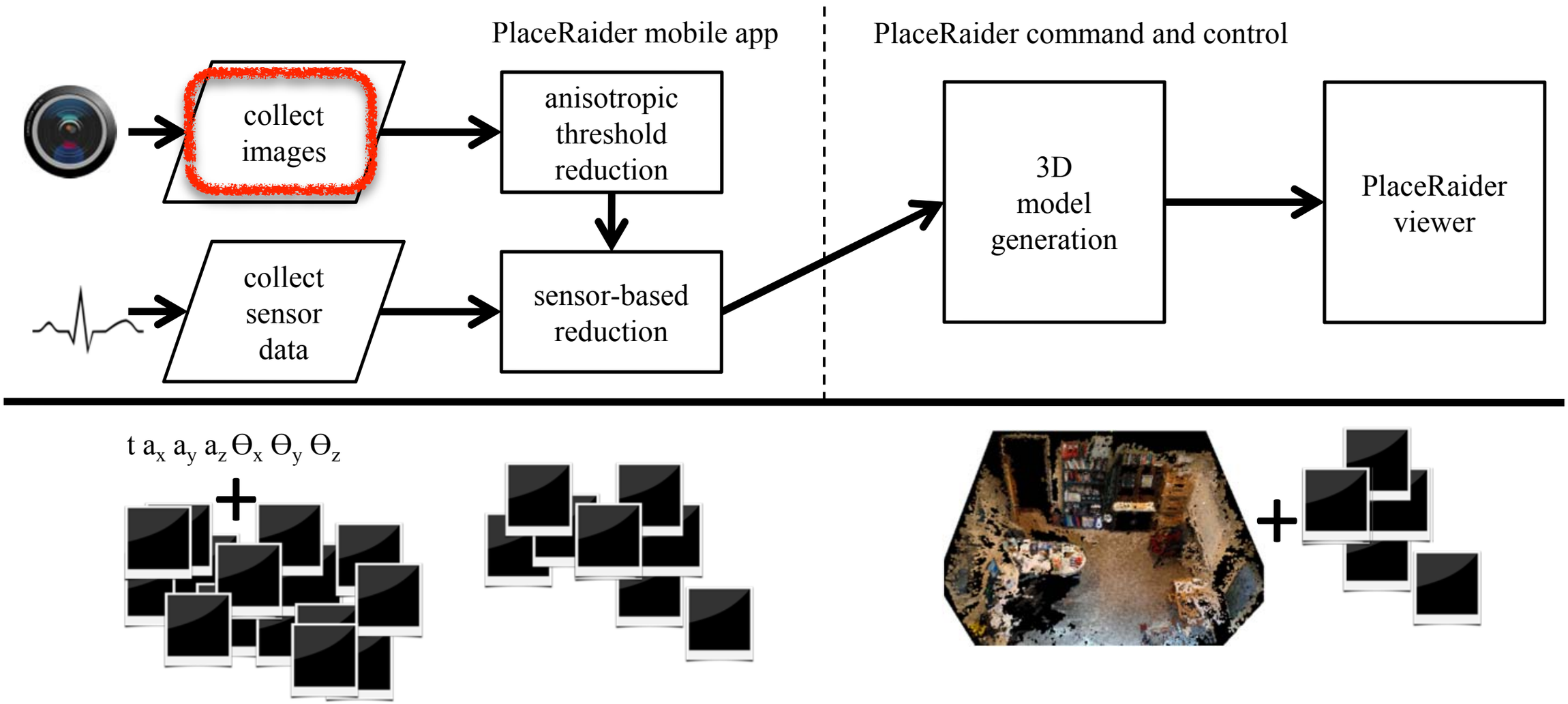


PlaceRaider Architecture

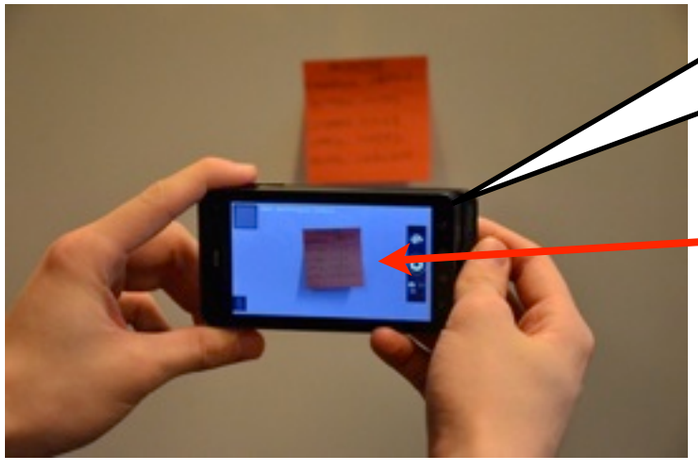
Navigating the model



Collecting Images



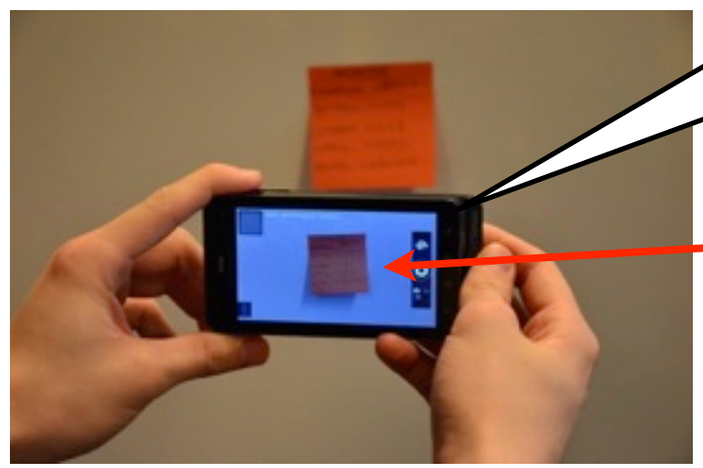
Disabling image previews and shutter sounds



Click

Image preview

Disabling image previews and shutter sounds

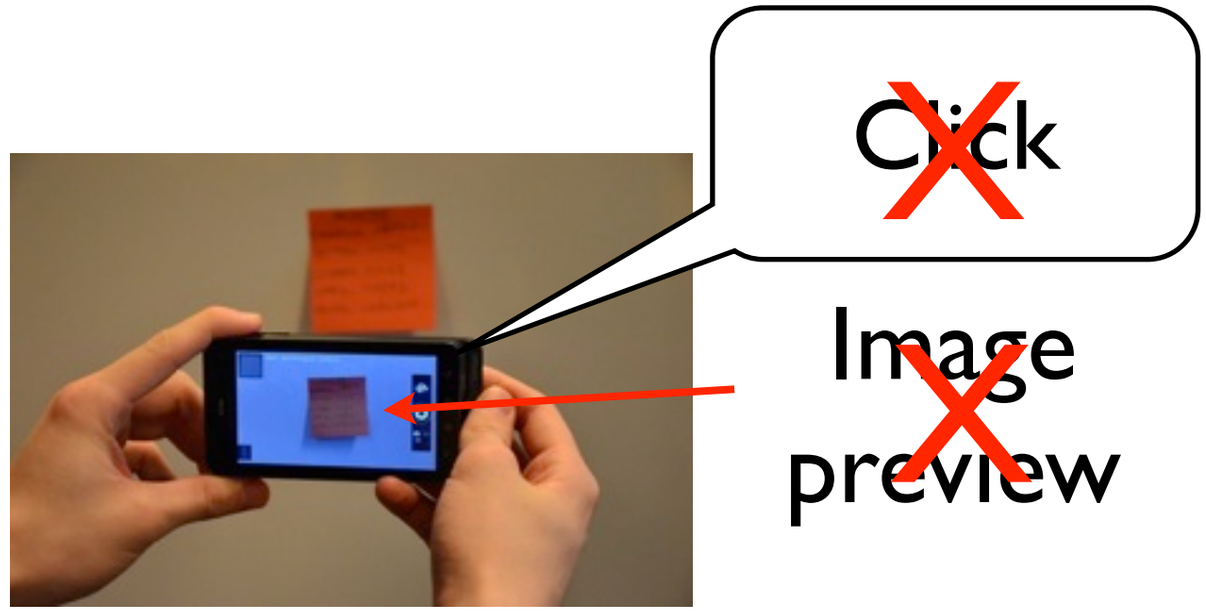


Click

Image preview

camera.setPreviewDisplay(null)

Disabling image previews and shutter sounds




```
camera.setPreviewDisplay(null)

AudioManager.setRingerMode(AudioManager.RINGER_MODE_SILENT)
camera.takePicture(null,null,jpegCallback);
AudioManager.setRingerMode(AudioManager.RINGER_MODE_NORMAL)
```

PlaceRaider Trojan requires innocuous permissions

PyDev – /Users/roberttempleman/Desktop/vandroid/AndroidManifest.xml – Eclipse – /Users/robertte...

Quick Access | PyDev | Resource | Team Synchronizing | Java | DDMS

Android Manifest Editor

```
<?xml version="1.0" encoding="utf-8"?>
<manifest xmlns:android="http://schemas.android.com/apk/res/android"
      package="remote.service"
      android:versionCode="1"
      android:versionName="1.0">
    <uses-permission android:name="android.permission.CAMERA"/>
    <uses-permission android:name="android.permission.INTERNET"/>
    <uses-permission android:name="android.permission.MODIFY_AUDIO_SETTINGS"/>
```

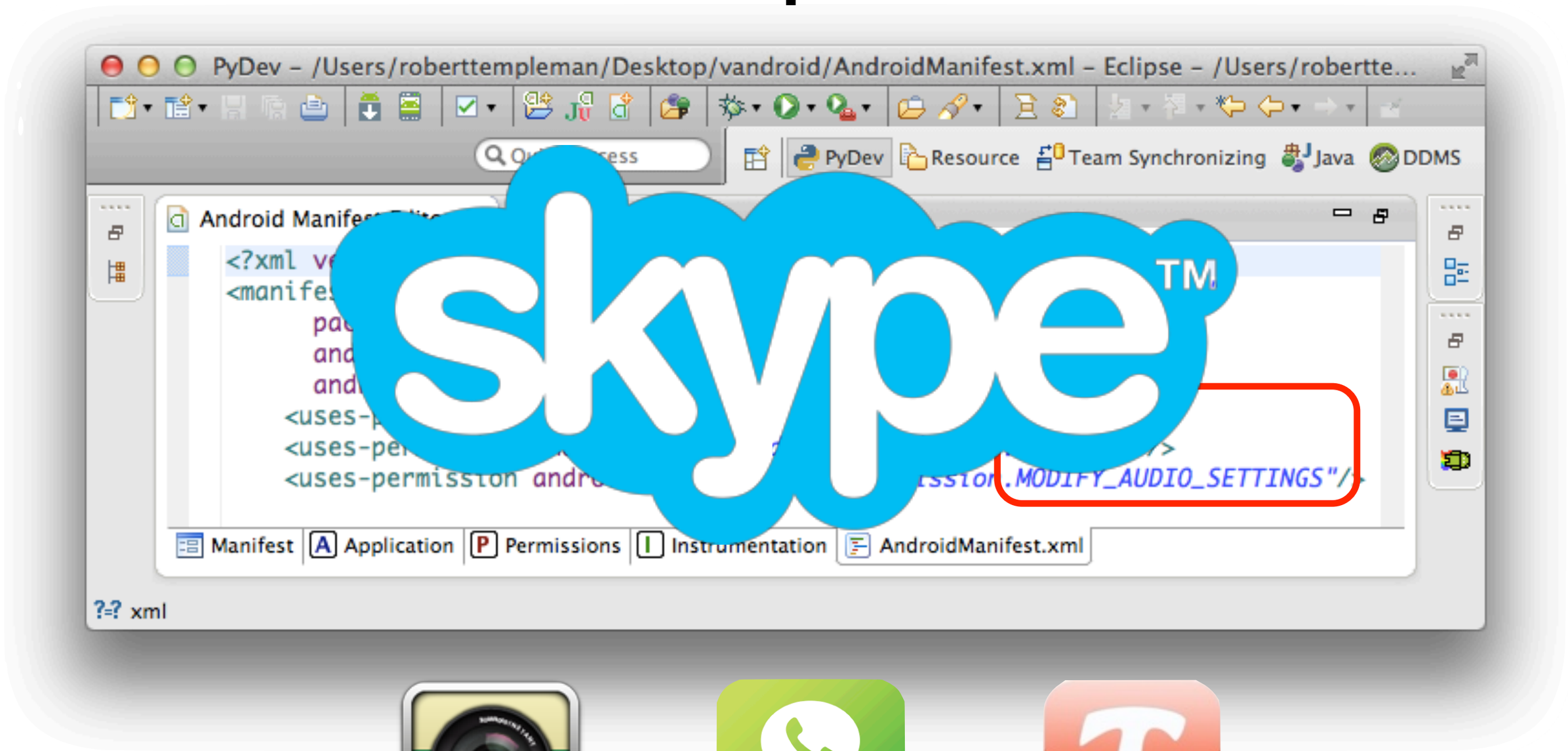
Manifest | Application | Permissions | Instrumentation | AndroidManifest.xml

?=? xml

NAVSEA WARFARE CENTERS CRANE

INDIANA UNIVERSITY

PlaceRaider Trojan requires innocuous permissions

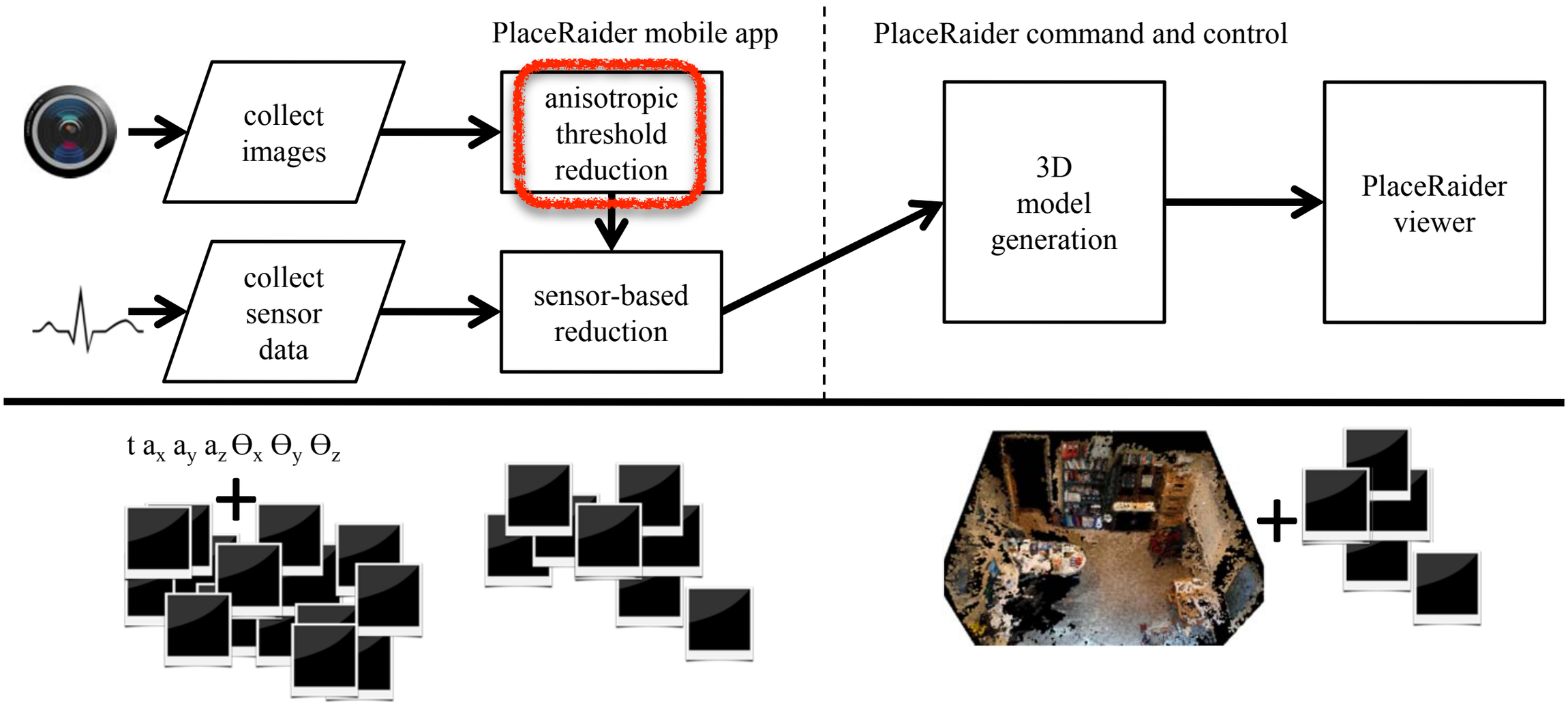


Retro Camera

LINE

Tango

Removing low-quality images



Removing low-quality images

Anisotropic analysis

(Gabarda and Cristobal 2007)

Variance in directional pixel entropy as a measure of image quality *or* ‘edginess’

Removing low-quality images

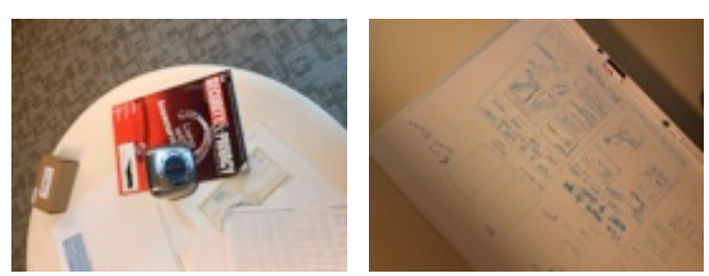
Anisotropic analysis

(Gabarda and Cristobal 2007)

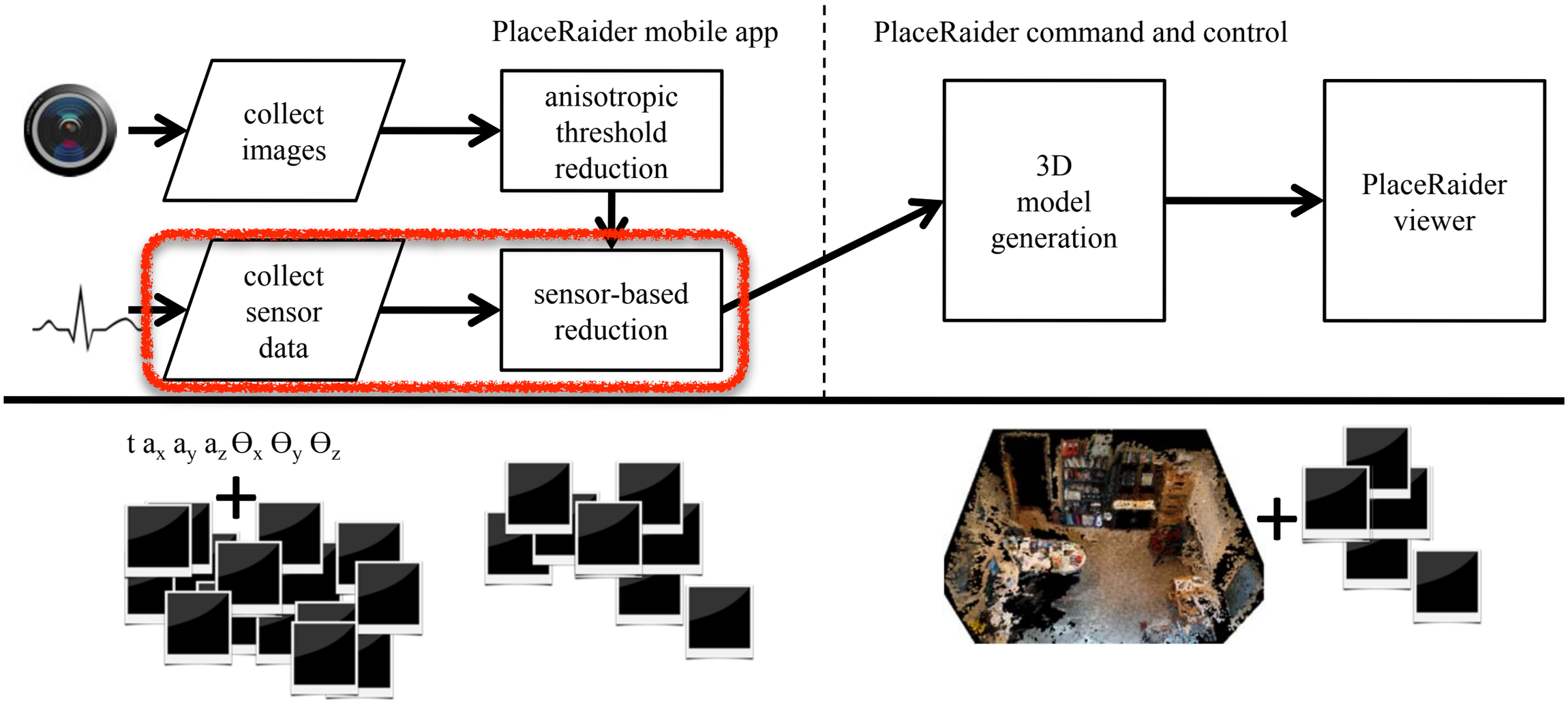
Variance in directional pixel entropy as a measure of image quality

or

'edginess'

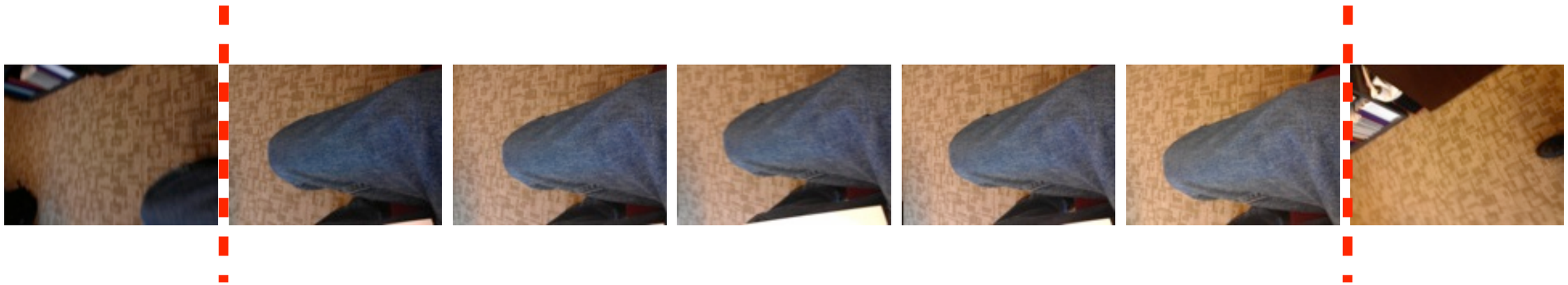


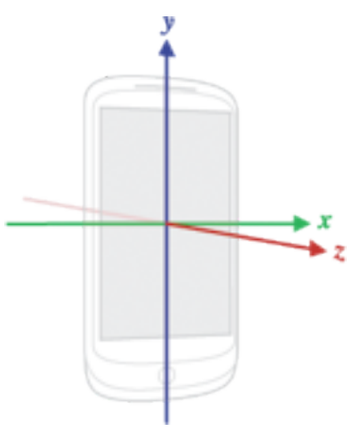
Guided removal of redundant images



Guided removal of redundant images

Movement-based reduction





developer.android.com

$\Theta_t = (\theta_x^t, \theta_y^t, \theta_z^t) \quad \Delta\Theta_t = \|\Theta_{t+1} - \Theta_t\|$

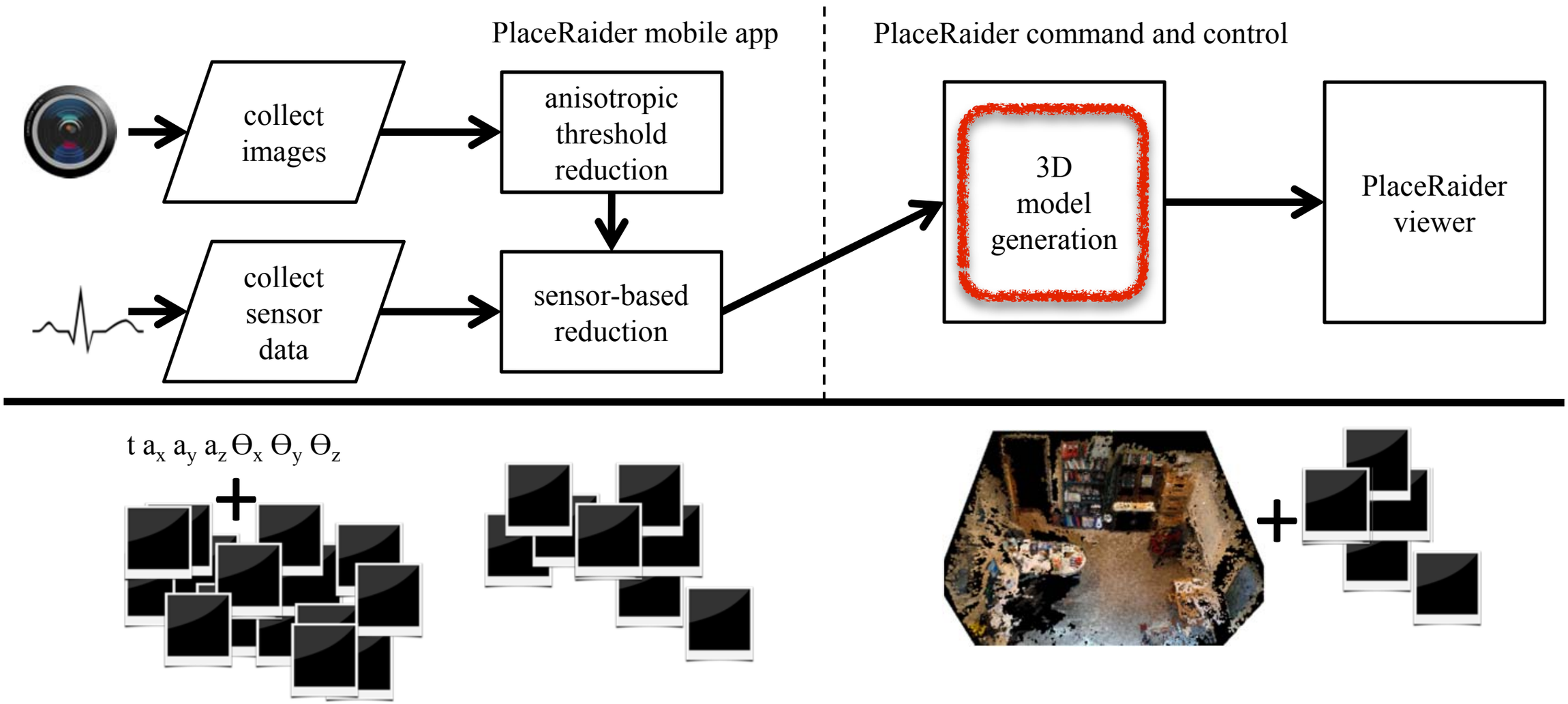
Identify sequences of images within some rotation threshold

Guided removal of redundant images

Movement-based reduction

Keep the image in each series with the highest anisotropic index

Building a 3D model



Building a 3D model

Bundler

sparse 3D reconstruction of camera and scene geometry

http://phototour.cs.washington.edu/bundler/

PMVS2

dense multi-view stereopsis

http://www.di.ens.fr/pmvs/

Bundler

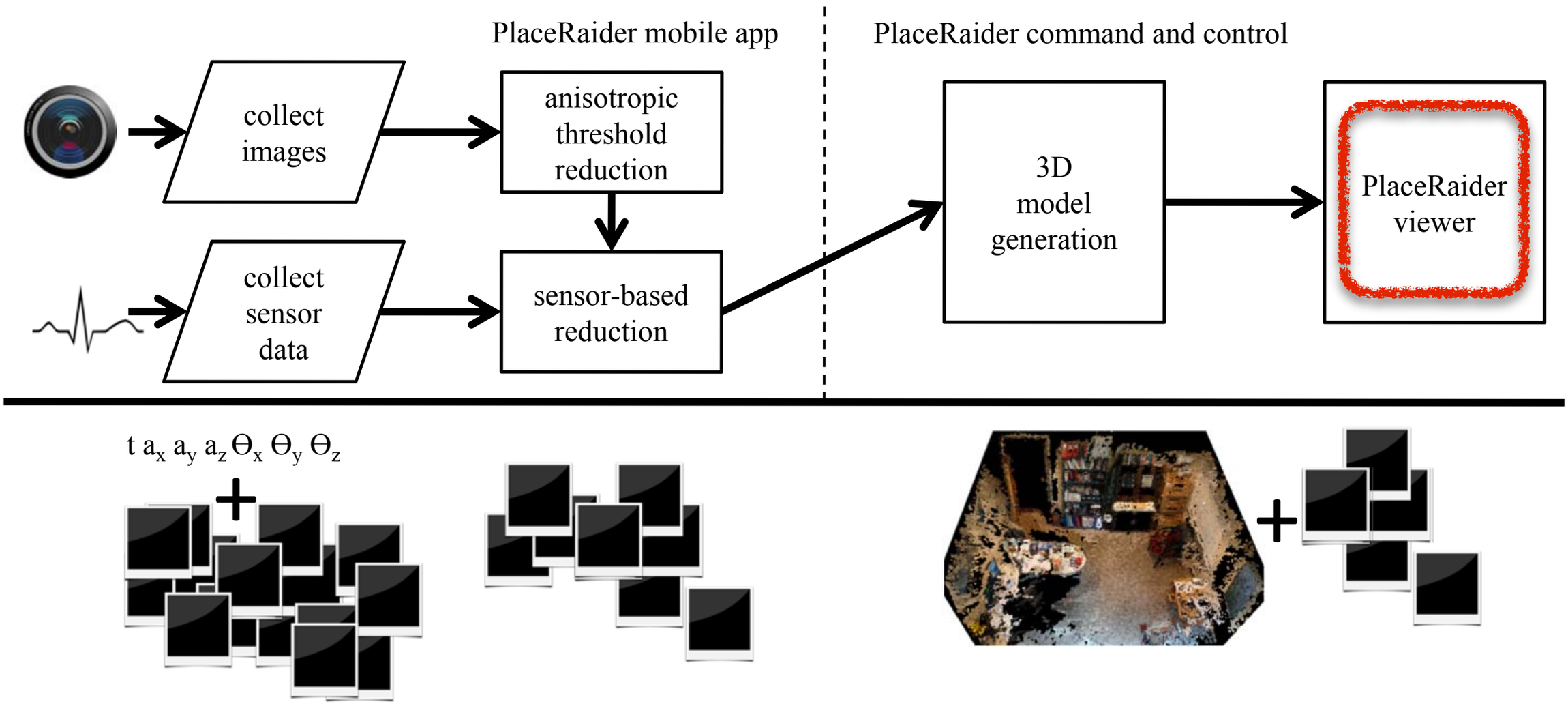
Sparse model

PMVS2

Dense model

PLY - polygon file format
PMVS - patch-based multi-view stereo

Navigating the Data



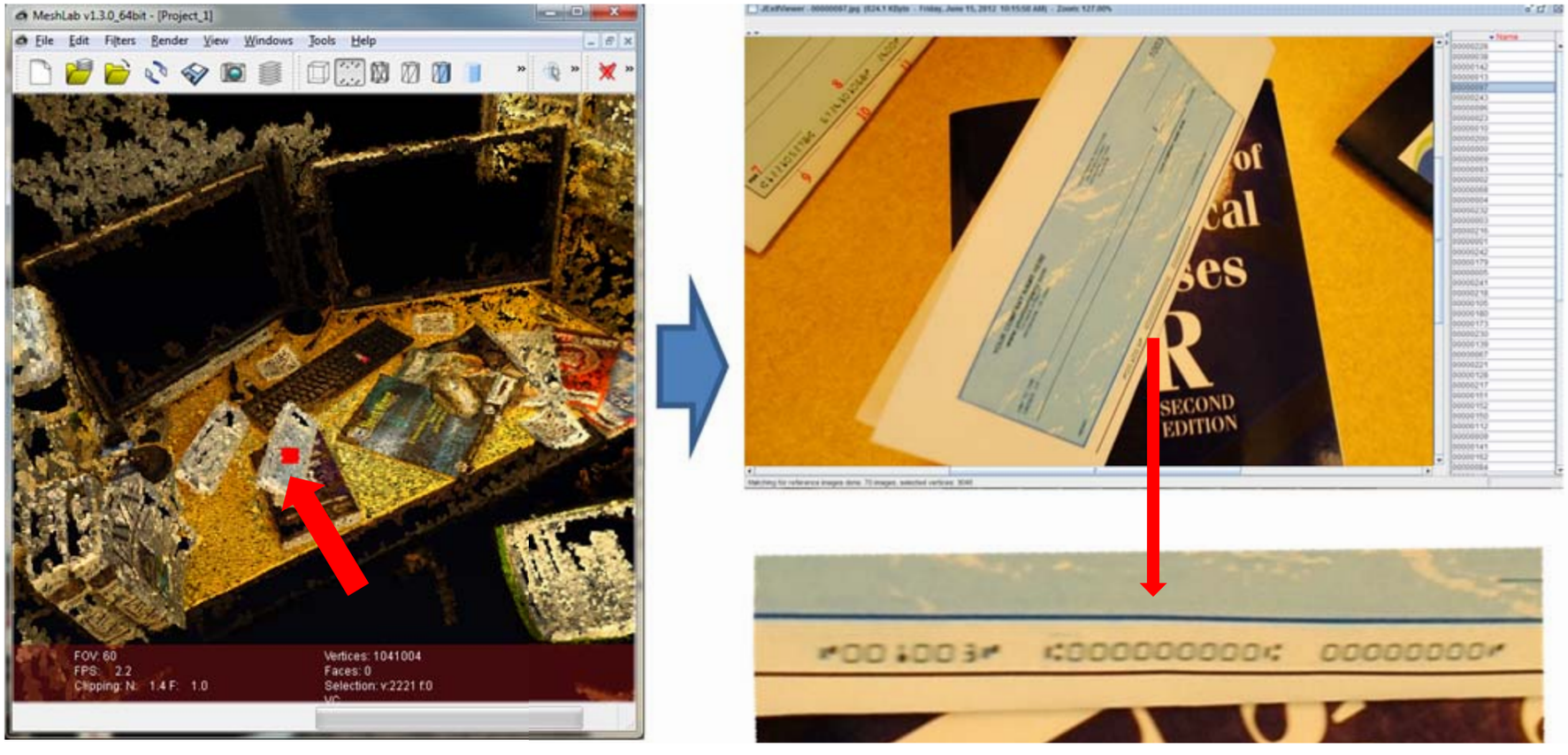
Navigating the Data

Meshlab - Point cloud (.PLY) viewer

custom plugin to select vertices and list contributing images

JExifViewer - image viewer integrated with plugin

explore and manipulate presented image sets



Evaluation

Study 1: Can we build 3D models from opportunistically collected photos?

20 participants
Android HTC Amaze phone
Surreptitious collection in lab

tests took ~20-45 minutes
μ_{images}=864/test

Tasks

1. **Please SIT in the swivel chair for the following activity:** Check the local weather on the browser (Perform a Google search for "47405 weather")
2. **Please SIT in the swivel chair for the following activity:** Go to the IDS News website and read no more than four paragraphs of the first article on the website (do not click through to other sites).
3. **While holding the phone:** Remove the folder from the bag and place it on the desk.
4. **Please SIT in the swivel chair for the following activity:** Hold the phone to your ear and pretend you are in a phone conversation for 3 minutes. You do not need to speak during this pretend call. It is okay to change positions of the phone during this pretend call (e.g., move the phone to another ear if you arm gets tired).
5. **Please STAND during the following activity:** Take a picture of the whiteboard.
6. **Please STAND during the following activity:** Put the phone in your pocket.
7. **Please WALK around the room for the following activity:** Pull the phone from your pocket, and pretend to have a 3 minute phone conversation as before. You do not need to speak during this pretend call. Walk naturally and comfortably through the room during this pretend call. It is okay to stop periodically if you are tired.
8. **Please SIT in the NON-swivel chair for the following activity:** Check the local weather again on the browser (Perform a Google search for "47405 weather")

NAVSEA WARFARE CENTERS CRANE

INDIANA UNIVERSITY

Examined 3D reconstructions for each participant's dataset

Model quality varied (partly a function of # of images)

Average reduction of 73.2% in # of images per test

http://www.youtube.com/watch?v=ItA791RGvrM

Study 2: Do these 3D models aid virtual theft?

3D group

N = 10

vs.

Raw group

N = 8

Coarse features - walls, doors, pieces of furniture, etc.

Fine features - checks, barcodes, monitors, whiteboard, etc.

PlaceRaider is useful for reconnaissance and exploration

Coarse features - 3D group performed better

Raw images: 5.8% of raw features correctly identified (σ = 45.8%)

3D model + viewer: 86% (σ = 10.2%)

(Welch's t-test, $p < 0.002$)

Fine features - no statistical significance between groups

People can visually process images at high rates, (20 images/second)

http://chronicle.com/article/From-Bench-to-Bunker-/132743/

But 3D models may perform better in larger reconstructions

Defending against sensory malware like PlaceRaider - it's complicated

www.mysecuritysign.com

OS-based defenses

Require a substantial **preview** surface object

Hardwire a **shutter sound** or add another hardware **indicator**

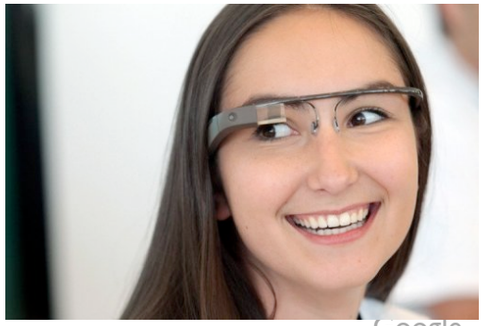
User driven access control
(Roesner et al., Oakland '12)

In conclusion...

Visual malware enables sophisticated reconnaissance and ‘virtual theft’

This threat is only amplified with augmented reality and first-person video applications

Memoto



Google

Need generalizable defenses to counter sensory malware

NAVSEA WARFARE CENTERS CRANE

NSF

INDIANA UNIVERSITY
SCHOOL OF INFORMATICS AND COMPUTING
Center for Security Informatics
Bloomington

NAVSEA
WARFARE CENTERS
CRANE

NSF

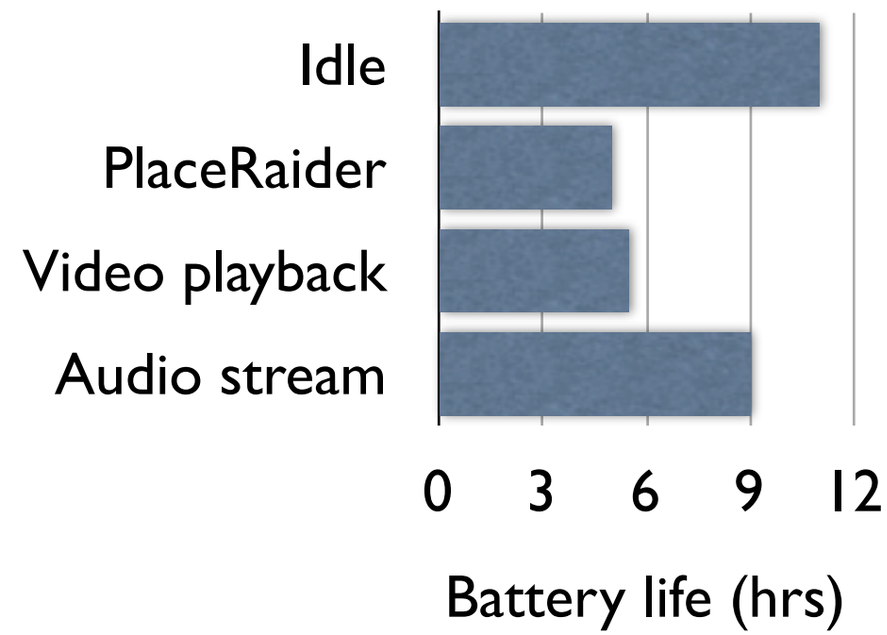
INDIANA UNIVERSITY
SCHOOL OF INFORMATICS AND COMPUTING
Center for Security Informatics
Bloomington

Backup Slides

Stealthiness of PlaceRaider

Power

At maximal collection rate (1800 photos/hr) power draw is comparable to other applications.
Tested on HTC Amaze.



Bandwidth

Transmit images only when connected to WiFi networks

Max image collection rate	1800 images/hr
Expected reduction	0.261
Avg file size (1MP)	0.138 MB/image
Avg data bandwidth	**64.83 MB/hr**

Current permissions are too loose

Fine-grained permissions are necessary!

Enck et al. (2009), Nauman et al. (2010), Felt et al (2011), Jeon et al. (2011)

Don't take pictures at work	Don't take pictures between 9PM and 3AM
Don't take pictures in bars	Don't take pictures in bathrooms
Don't take pictures of my monitor	Don't take pictures of me in Vegas
Only take pictures that I command	Don't take pictures of me naked