On Limitations of Access Control Models for Privacy-Sensitive Sensors

Giuseppe Petracca
Ph.D. Candidate
gxp18@cse.psu.edu

Advisor: **Dr. Trent Jaeger**
Dept. of Computer Science and Engineering
Institute for Networking and Security Research
The Pennsylvania State University

Agenda

PennState

- Old Classic Computer Systems vs Today’s Computer Systems
- Classic Access Control Models
- Why Today’s World is Different (Demos)
  - Audio Channels
  - Continuous-Sensing Sensors
  - Audio-Visual Sensors
- Limitations of classic/contemporary Access Control Models
- Contributions from our INSR (SIIS) Research Lab

Old Classic Computer Systems

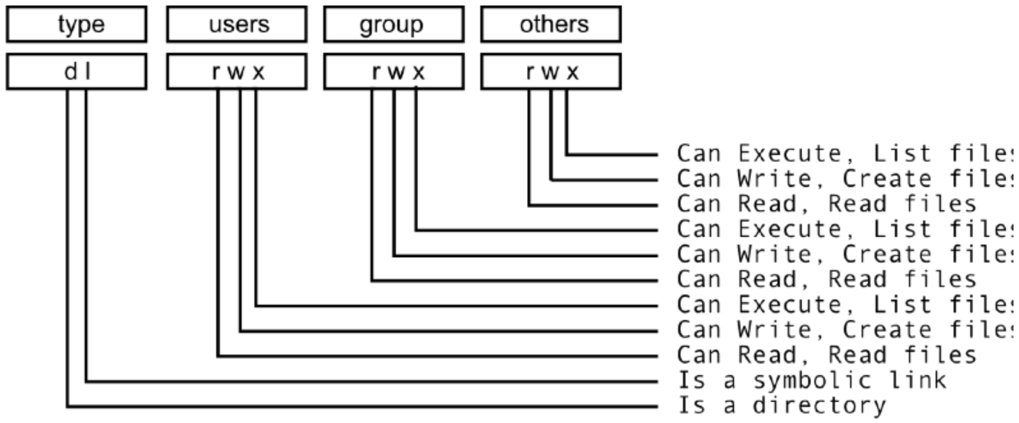
Today’s Computer Systems

They can measure and sense the **Physical World**!

Classic Access Control Models

Discretionary Access Control (DAC)

The data owner determines who can access specific resources (i.e., Unix File Permission)



Role-Based Access Control (RBAC)

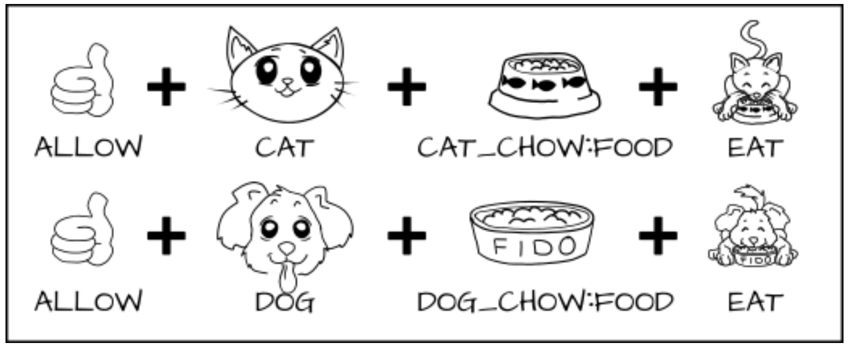
Users are allowed to access resources based on the job title (or role)

Attribute-Based Access Control (ABAC)

Rights are granted to users through the use of policies which combine attributes together

Mandatory Access Control (MAC)

Users do not have freedom to determine who has access to their files/objects (i.e., SELinux)



Today's World is Different!

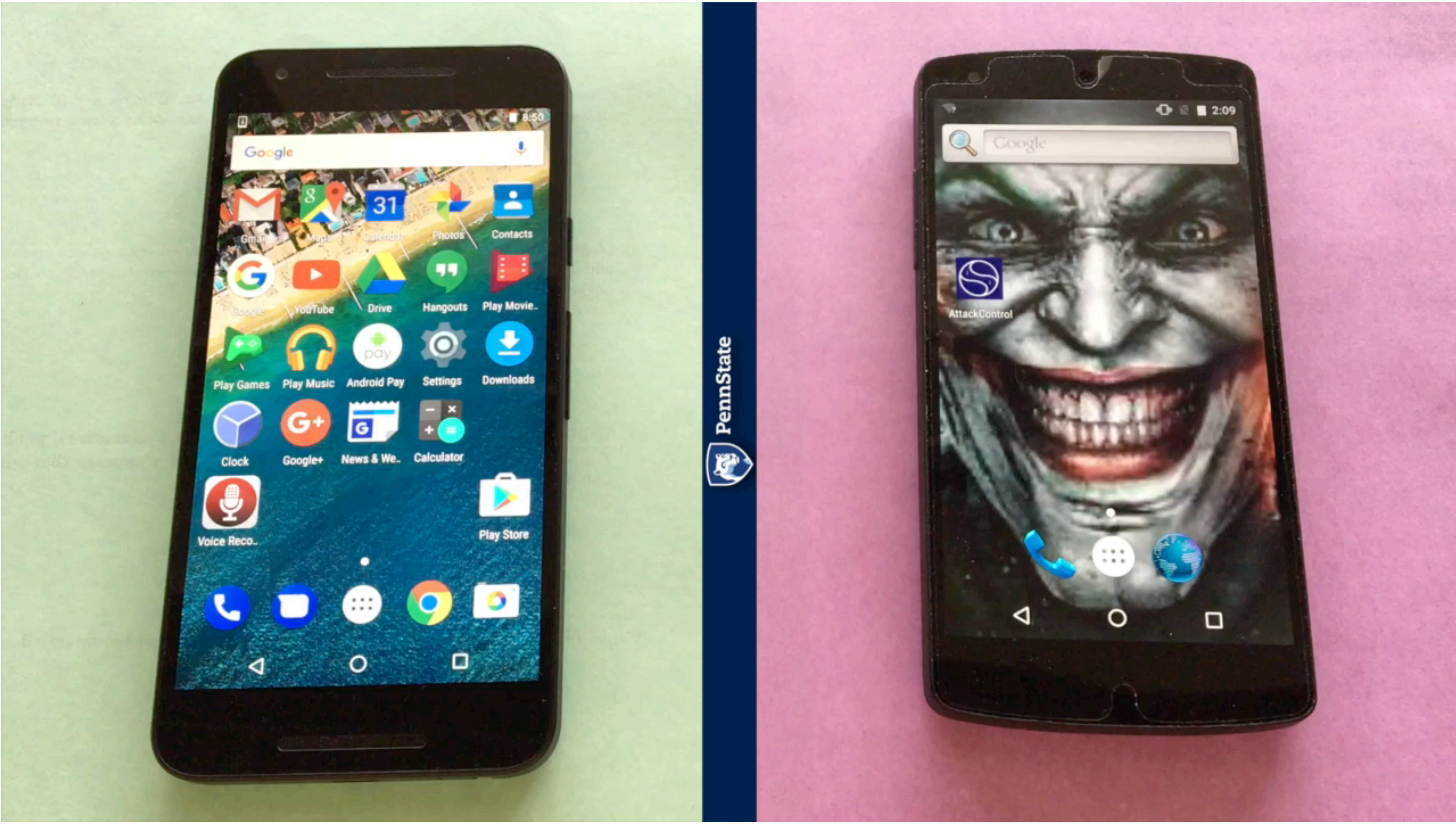
State College, PA

(44.2 miles)

Altoona, PA

What could go **Wrong**?

Exploitation of Audio Channels



State College, PA

Altoona, PA

Exploitation of Audio Channels

This is not a new issue!

Who is interested in eavesdropping my voice?

This is a very specific scenario!

Exploitation of Audio Channels

PennState

Inaudible Sound as a Covert Channel in Mobile Devices

Luke Deshotels
North Carolina State University
alecdeshotels@gmail.com

FTC Issues Warning Letters to App Developers Using 'Silverpush' Code

Letters Warn Companies of Privacy Risks In Audio Monitoring Technology

FOR RELEASE

March 17, 2016

Bridging the Air Gap: Inaudible Data Exfiltration by Insiders

Completed Research Paper

Samuel Joseph O'Malley
University of South Australia
omalsa04@gmail.com

Kim-Kwang Raymond Choo
University of South Australia
raymond.choo@unisa.edu.au

Lawsuit claims popular Warriors app accesses phone's microphone to eavesdrop on you

By Katie Dowd, SFGATE Updated 3:13 pm, Thursday, September 1, 2016

SAN FRANCISCO — Want to invisibly spy on 10 iPhone owners without their knowledge? Gather their every keystroke, sound, message and location? That will cost you $650,000, plus a $500,000 setup fee with an Israeli outfit called the NSO Group. You can spy on more people if you would like — just check out the company's price list.

16. Februar 2017, 21:15 Uhr Überwachung im Kinderzimmer

Netzagentur ruft Eltern auf, Puppe "Cayla" zu zerstören

Continuous-Sensing Sensors

GPS Wi Fi™ 3G

Why are these devices a **Threat** for our **Privacy**?

Continuous-Sensing Sensors

PennState

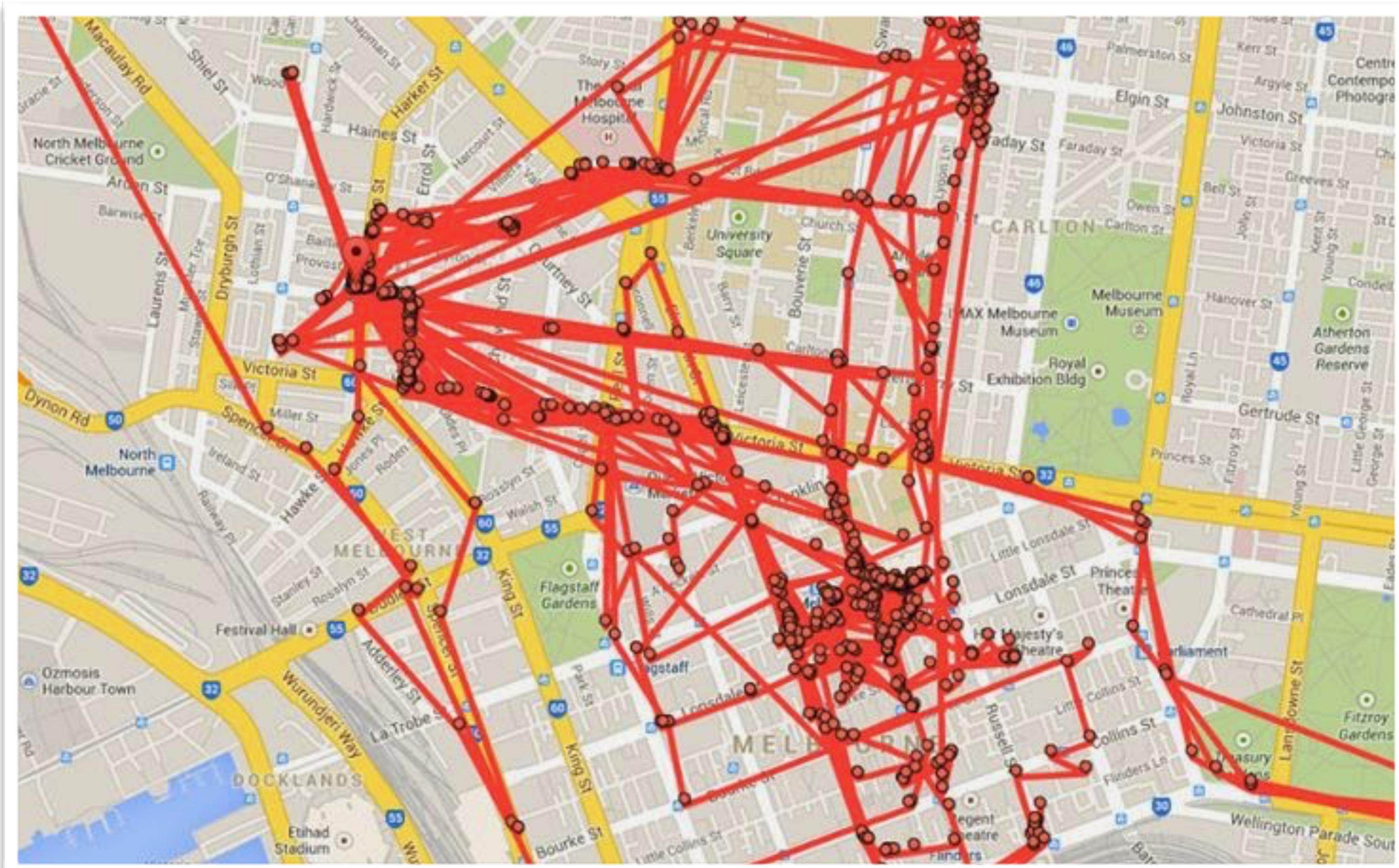
Privacy Concerns raising from **Inference Attacks** on Sensed Location Data

Let's assume a third party has access to **Location Data Points**
(timestamped latitude and longitude coordinates)
from a GPS or Wi-Fi receiver on the victim's platform (i.e., smartphone)

What can a **Cybercriminal** do with such **Data**?

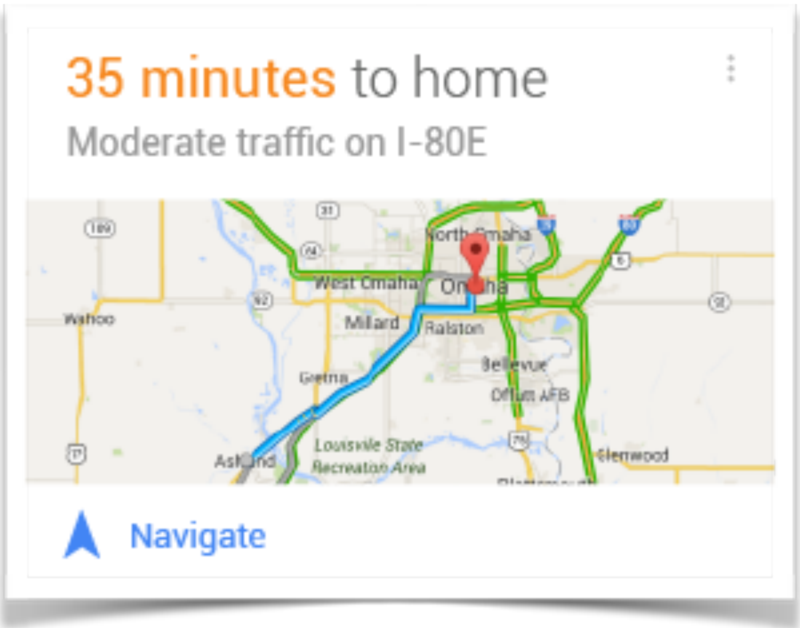
Continuous-Sensing Sensors

PennState

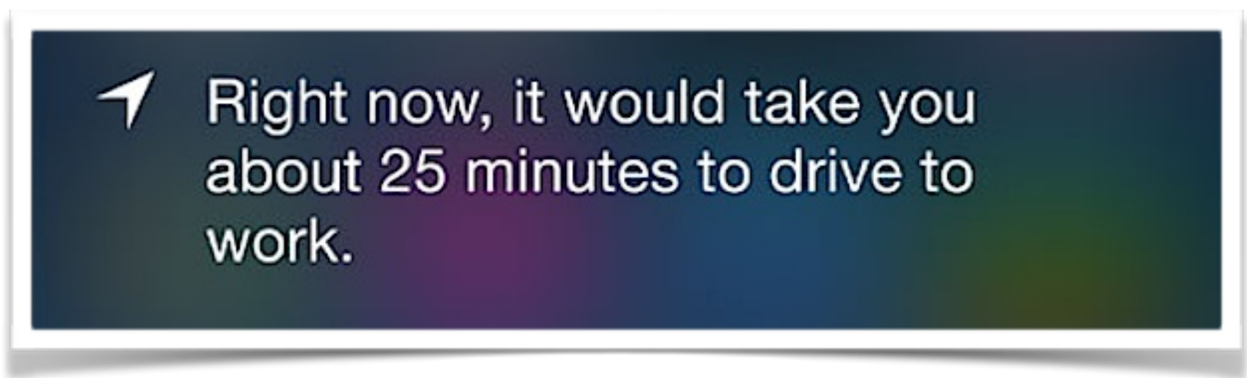


Rupert Murdoch labeled Google worse than the NSA, saying “NSA privacy invasion bad, but nothing compared to Google.”

Is Google the only Evil?



Drive safe! your best buddy Google Now.



Sincerely, your best friend iOS10!

What if this **Data** is available to **Cybercriminals**?

Inference Attacks on Sensed Location Data

PennState

Heuristics Available to the Adversary

- First and Last Daily Destination
- Most Stationary Way Points
- Larger Clusters
- Best Time (Sleep Time and Work Time)

Credit: "Inference Attacks on Location Tracks" [Krumm, Pervasive 2007]

CampusLife Data Set

Over 483k time-stamped location data points

GPS and Wi-Fi signals around the University Park Campus

4 weeks for 24 hours/day

All movements performed by a graduate student working on campus and living off campus (http : //sites.psu.edu/petracca/campuslife/)

	First/Last Destination	Most Stationary	Larger Clusters	Best Time
Home	**96.43%**	**96.43%**	**96.43%**	**89.26%**
Work	**78.57%**	**71.43%**	**75%**	**71.43%**

Inference Attacks on Sensed Data

PennState

Gyrophone: Recognizing Speech From Gyroscope Signals

Yan Michalevsky Dan Boneh
Computer Science Department
Stanford University

Gabi Nakibly
National Research & Simulation Center
Rafael Ltd.

(sp)iPhone: Decoding Vibrations From Nearby Keyboards Using Mobile Phone Accelerometers

Philip Marquardt*
MIT Lincoln Laboratory
244 Wood Street, Lexington, MA USA
philip.marquardt@ll.mit.edu

Arunabh Verma, Henry Carter and Patrick Traynor
Georgia Institute of Technology
{arunabh.verma@, carterh@, traynor@cc.}gatech.edu

ACCessory: Password Inference using Accelerometers on Smartphones*

Emmanuel Owusu, Jun Han, Sauvik Das, Adrian Perrig, Joy Zhang
{eowusu, junhan, sauvik, perrig, sky}@cmu.edu
Carnegie Mellon University

TapLogger: Inferring User Inputs On Smartphone Touchscreens Using On-board Motion Sensors

Zhi Xu
Department of Computer Science and Engineering
Pennsylvania State University
University Park, PA, USA
zux103@cse.psu.edu

Kun Bai
IBM T.J. Watson Research Center
Hawthorne, NY, USA
kunbai@us.ibm.com

Sencun Zhu
Department of Computer Science and Engineering
Pennsylvania State University
University Park, PA, USA
szhu@cse.psu.edu

Audio-Visual Sensors

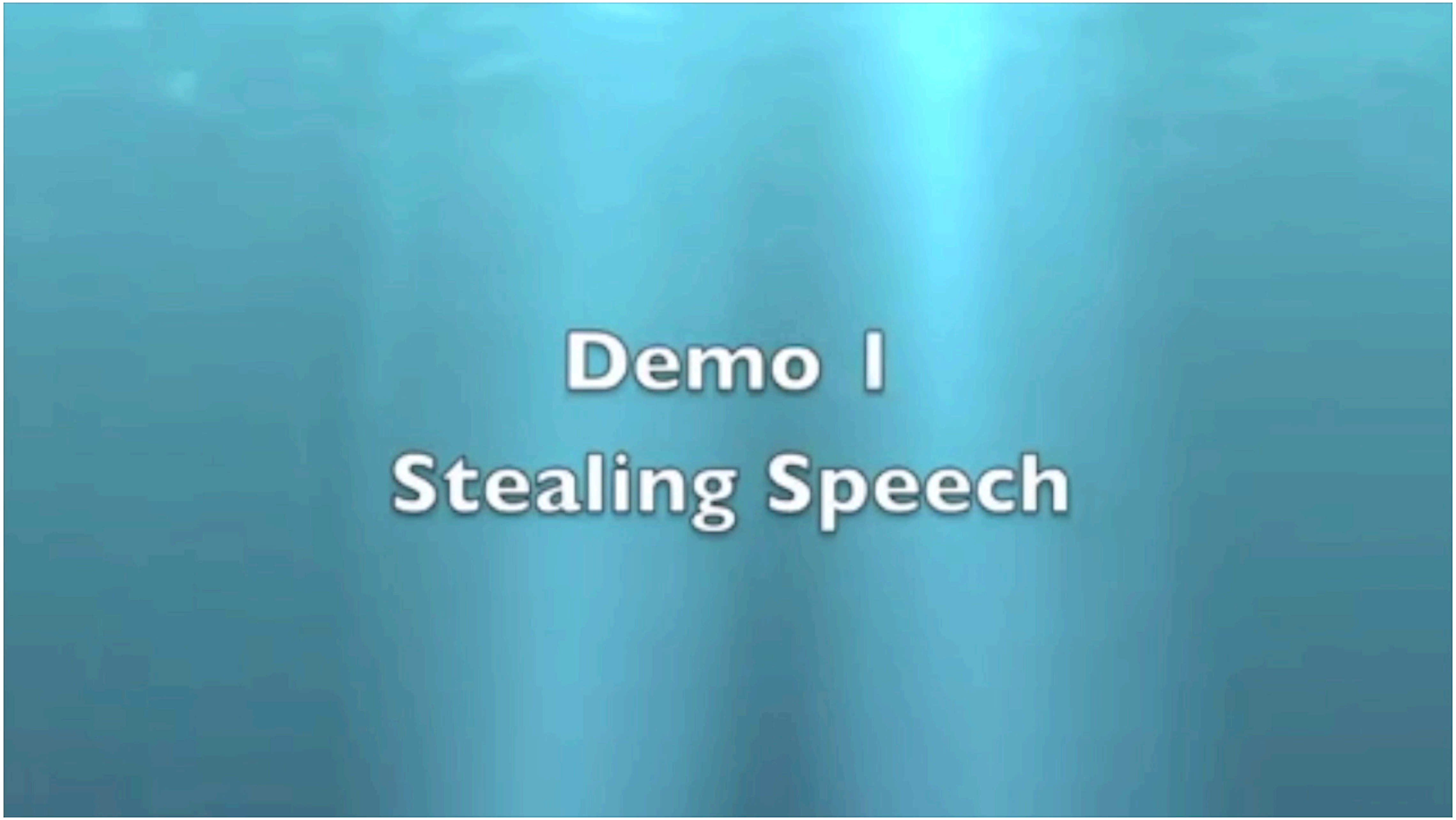
Cameras

Microphone

Why aren't **Permission-Based** solutions sufficient?
What could go **wrong**?

Exploitation of Audio-Visual Sensors

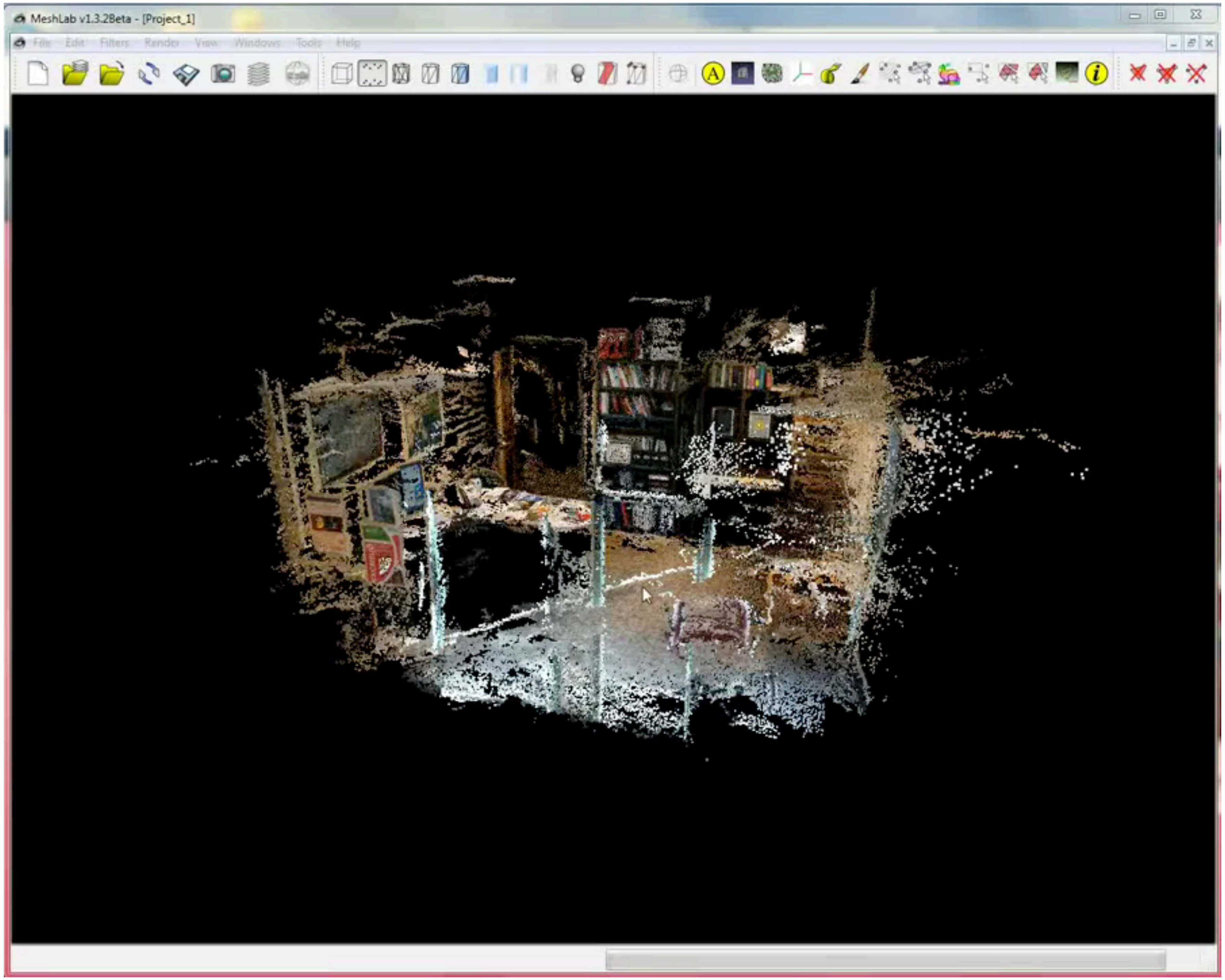
Secretly records your voice to retrieve sensitive information, such as your Credit Card Number!



Credit: *Apu Kapadia et al.* (Researchers from the school of Informatics and Computing at Indiana University in Bloomington)

Exploitation of Audio-Visual Sensors

Secretly record your environment and reconstruct it as a 3D virtual model for a malicious user to browse!



Credit: *Apu Kapadia et al.* (Researchers from the school of Informatics and Computing at Indiana University in Bloomington)

Contributions from our INSR (SIIS) Research Lab

PennState

Preventing attacks on **Audio Channels**

AuDroid: Preventing Attacks on Audio Channels in Mobile Devices

Giuseppe Petracca, Yuqiong Sun, and Trent Jaeger
Dept. of Computer Science and Engineering
The Pennsylvania State University
{gxp18, yus138, tjaeger}@cse.psu.edu

Ahmad Atamli
Dept. of Computer Science
University of Oxford
atamli@cs.ox.ac.uk

ACSAC'15

Preventing inference attacks on **Sensed Location Data**

Agility Maneuvers to Mitigate Inference Attacks on Sensed Location Data

Giuseppe Petracca
gxp18@cse.psu.edu
Computer Science and Engineering
The Pennsylvania State University

Lisa M. Marvel
marvel@ieee.org
Ananthram Swami
ananthram.swami.civ@mail.mil
Army Research Laboratory

Trent Jaeger
tjaeger@cse.psu.edu
Computer Science and Engineering
The Pennsylvania State University

MILCOM'16

Preventing adversarial use of **Privacy-Sensitive Sensors**

AWARE: Preventing Abuse of Privacy-Sensitive Sensors via Operation Bindings

Giuseppe Petracca[1], Ahmad-Atamli Reineh[2], Yuqiong Sun[1], Jens Grossklags[3], and Trent Jaeger[1]

Under Submission

I N S R

ARL

Limitation of Current Access Control Models

Unable to Identify Dynamically-Created Audio Channels

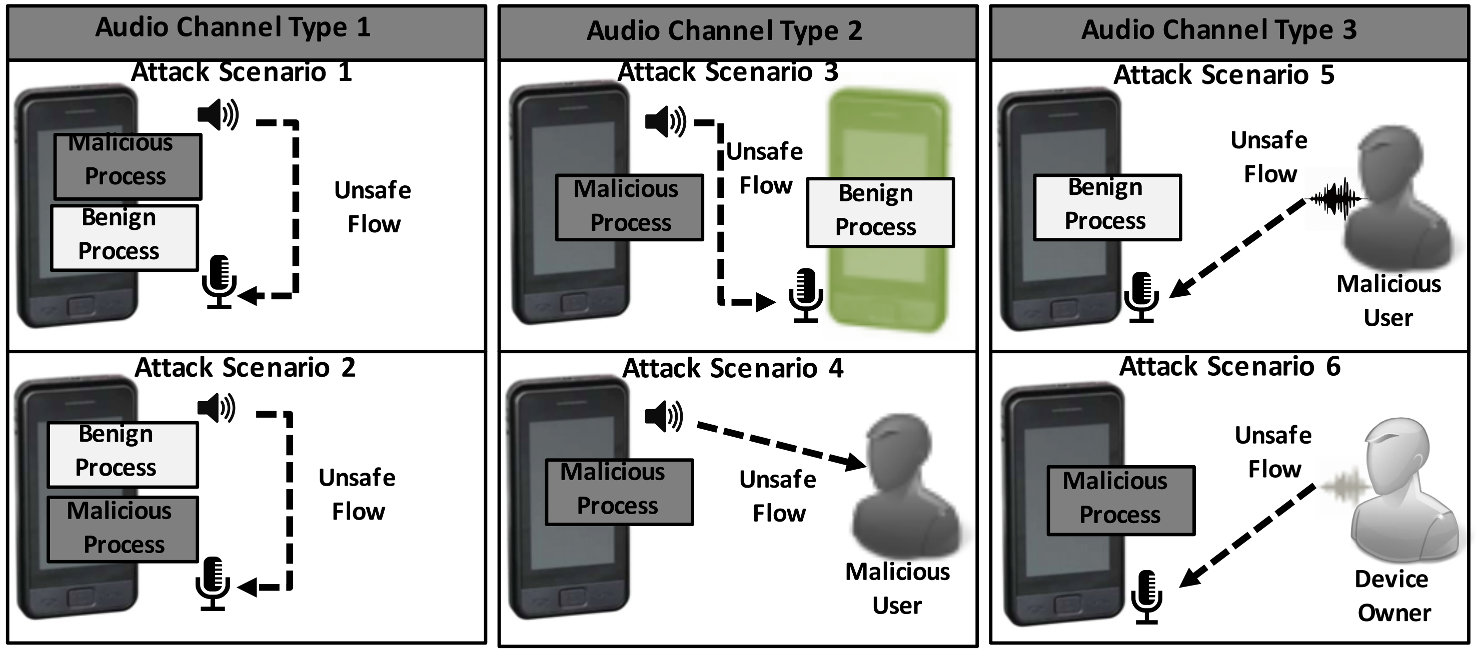
Preventing Attacks on Audio Channels

Communication Channels conveying Audio Signals

- 2 Endpoints (Microphone and Speaker)
- May involve **External Parties**
  - 3 Types of Audio Channels
  - **Eavesdropping** and **Confused Deputy** attacks

[Diao *et al.* SPSM'14]

[Jang *et al.* CCS'14]



[Keylogger] [Speak Out] [Schlegel *et al.* NDSS'11]

Confused Deputy

Eavesdropping

Preventing Attacks on Audio Channels

Static Labels for Internal Parties (Processes)

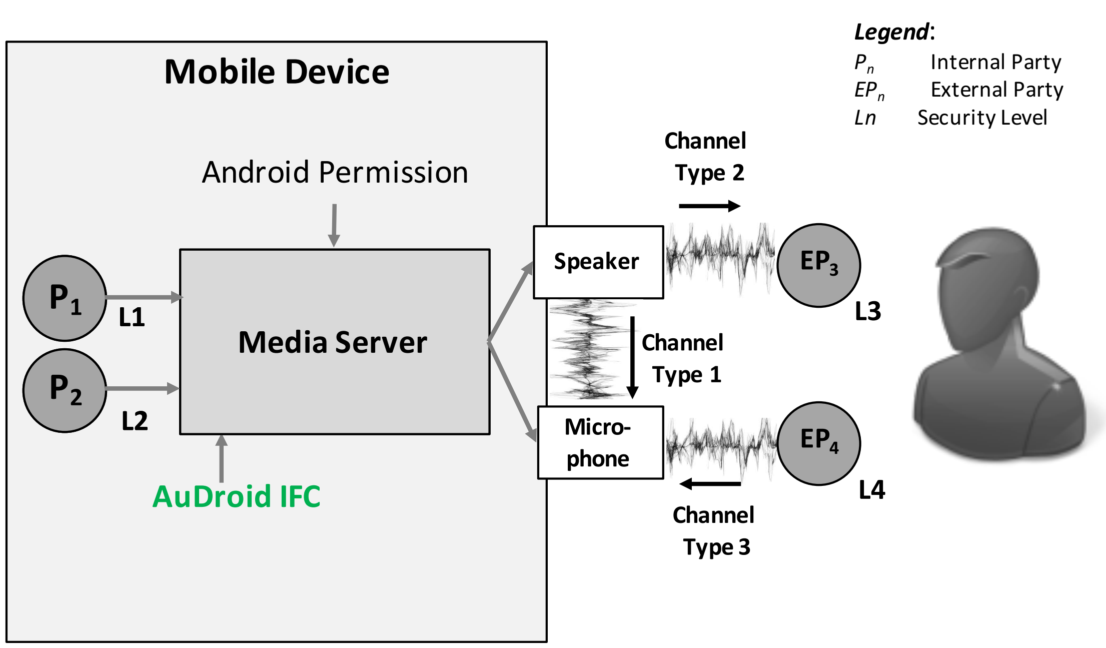
- PID
- Market Apps - Low Secrecy Low Integrity (LS,LI)
- System Apps and Services - High Secrecy High Integrity (HS, HI)

Dynamic Labels for Channels

- Two endpoints - Label depends on who controls endpoint

Dynamic Labels for External Parties (Other Devices or Users)

- Initial Label (Speaker – LS, HI) (Microphone – HS, LI)
- After Device Owner Authentication (HS, HI)



Preventing Attacks on Audio Channels

PennState

Prevention of **Unsafe Information Flows**:

- No flow from High-Secrecy Party to Low-Secrecy Party (***Bell–LaPadula***)
- No flow from Low-Integrity Party to High-Integrity Party (***Biba***)
- No flow among Low-Secrecy Low-Integrity Party (***Isolation*** of Apps)

Negligible **Performance Overhead** (order of microseconds per single access)

Compatible with existing application (Tested 17 widely-used Apps)

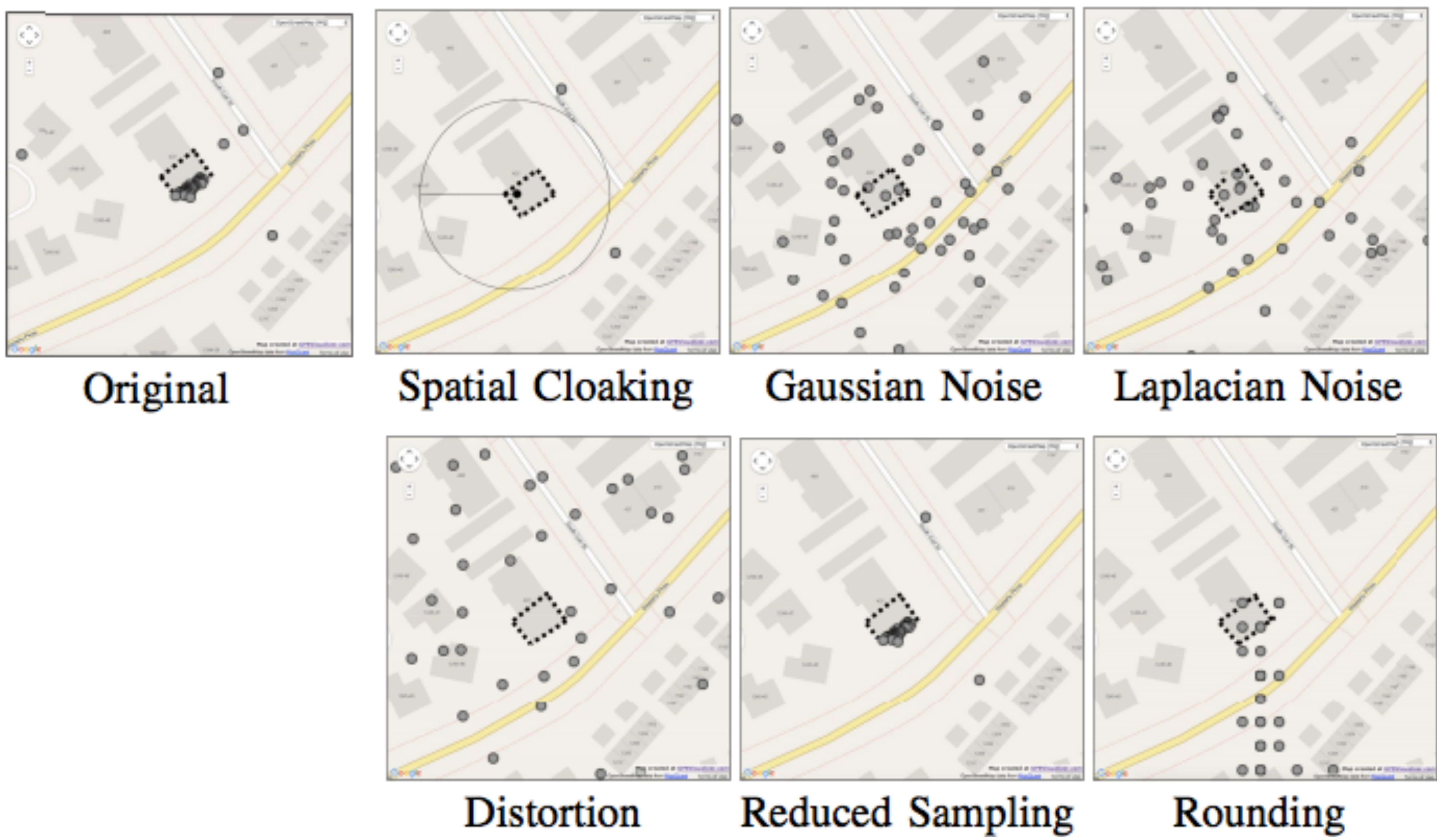
Preventing Inference Attacks on Sensed Data

Limitation of Current Access Control Models

Unable to Identify Malicious vs Benign use of Sensed Data

Preventing Inference Attacks on Sensed Data

Location Privacy-Preserving Mechanisms



Preventing Inference Attacks on Sensed Data

Black-Box Attacks

- The adversary has access to all location data points (timestamped longitude and latitude) produced by GPS and Wi-Fi receivers on the victim's mobile platform.

White-Box Attacks

- The adversary also knows the mechanisms used to protect the location data and the parameters used to configure such protection mechanisms.
- Example: (Spatial Cloaking) Radius of the circular area around sensitive locations.
- How would LPPMs perform in White-Box Attacks?

Preventing Inference Attacks on Sensed Data

PennState

Random Obfuscation

- ***Randomly*** select a protection mechanism from the set of available mechanism every time the sensed data **becomes stationary**

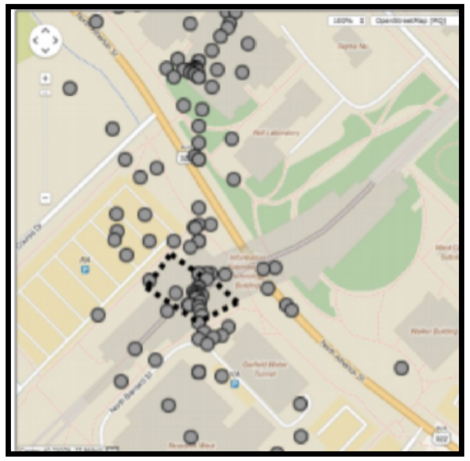
Spatial Uniform Distribution

- ***Uniformly*** distribute data points in the space of reading by adding ***Synthetic Data*** whenever the victim location **becomes stationarity** for a certain time period

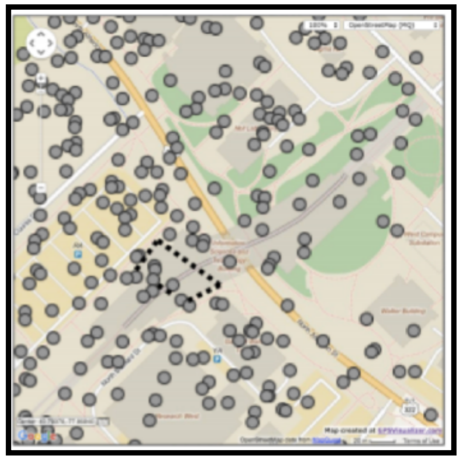
Temporal Uniform Distribution

- ***Uniformly*** distribute data points in the space of reading by adding ***Synthetic Data*** in ***interleaved time frames*** with the original data points

Original



Random



Spatial

Temporal

Preventing Inference Attacks on Sensed Data

Random Obfuscation

- Performs better (14.04% less) than most analyzed LPPMs - Randomness
- Slightly less effective for White-Box attacks (42.40% on avg.) compared to Black-Box Attacks (40.05% on avg.)

Spatial and Temporal Distribution

- Outperform state-of-the-art LPPMs (34.67% less for Black-Box and 52.02% less for White-Box Attacks)
- Stable even in White-Box attacks
- (Uniform Distribution) Each choice has exactly the same probability to be the original data point

Limitation of Current Access Control Models

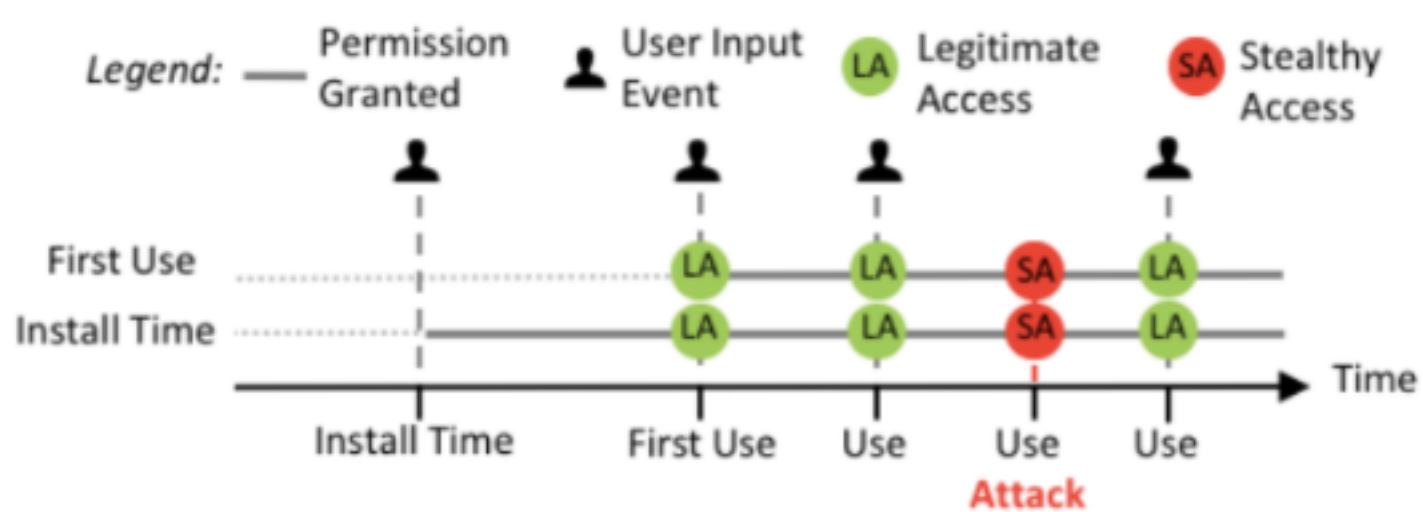
Unable to Enforce Contextual Use of Privacy-Sensitive Sensors

Preventing Misuse of Privacy-Sensitive Sensors

PennState

Permission-Based Systems

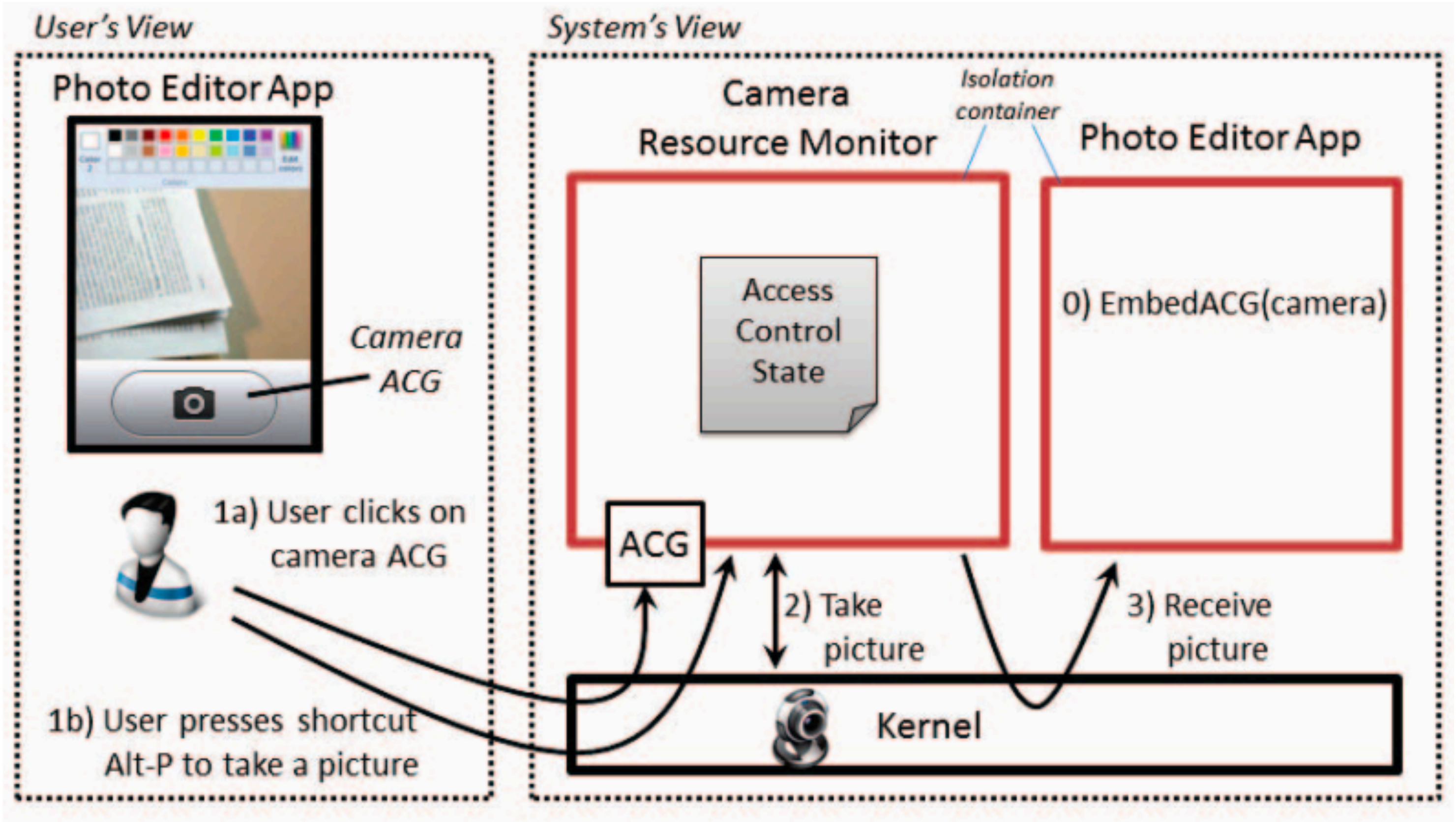
Apps can access sensitive-sensors (Cameras, Microphones and Screen Buffers) **at any time** after the user has authorized them at install time or at first use



Preventing Misuse of Privacy-Sensitive Sensors

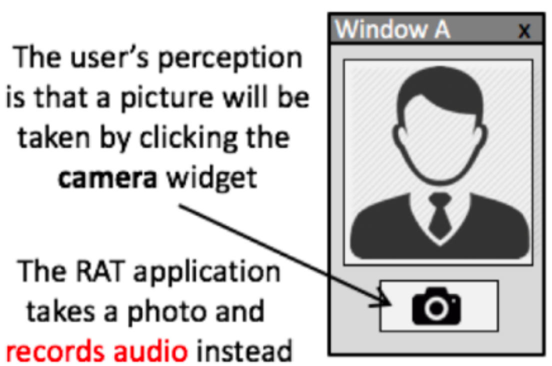
Access Control Gadgets (ACGs)

User-Driven Access Control by Roesner *et al*.

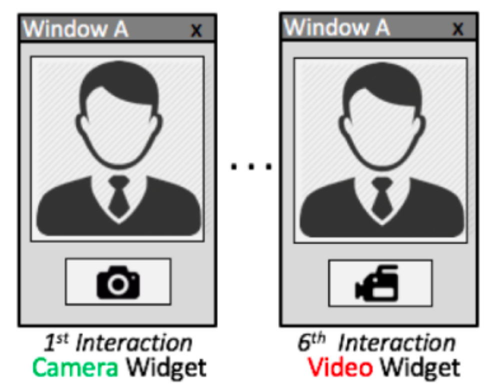


Preventing Misuse of Privacy-Sensitive Sensors

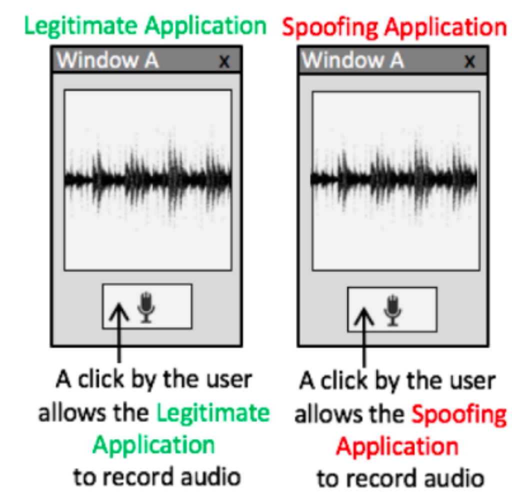
Adversarial Accesses leveraging the user as weak point!



Operation Switching



Bait-and-Switch



Identity Spoofing

Preventing Misuse of Privacy-Sensitive Sensors

We propose to leverage a strong **Operation Binding** and a **Display Context**

(Activity Window Call Graph)

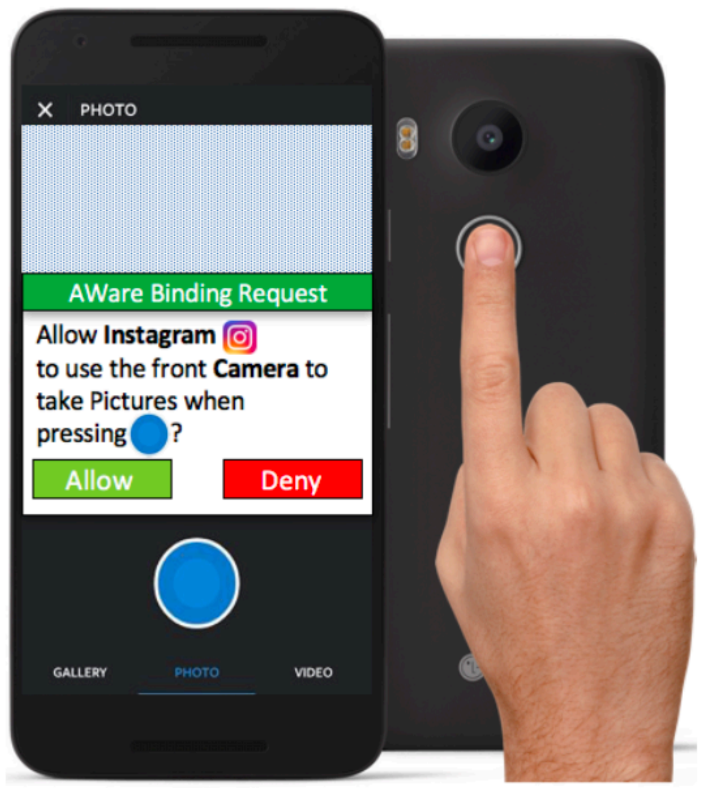


Figure 8: AWare *Binding Request* prompted to the user on the mobile platform's screen at *Operation Binding* creation. The app's identity is proved by the name and the graphical mark. A virtual blind cover the camera preview until authorization. For better security, in mobile platforms equipped with a fingerprint scanner, AWare recognizes the device owner's fingerprint as the only authorized input for creating a new *Operation Binding*.

User-Initiated - Explicit User Authorization - Low User Effort

Preventing Misuse of Privacy-Sensitive Sensors

Leverage **On-Screen Notifications** to Users

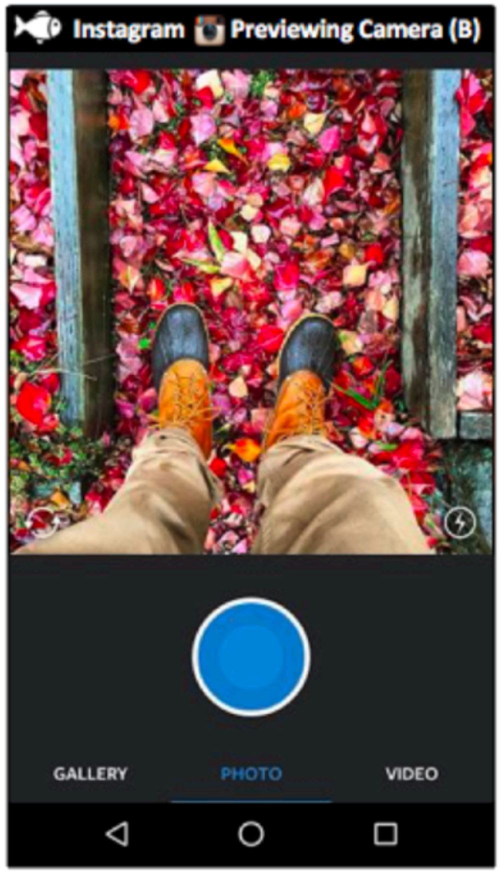


Figure 10: AWARE *security message* displayed on the mobile platform's status bar notifying the user that the Instagram application is previewing the back camera (B) for pictures. The security companion (white fish) aids the user in verifying the authenticity of the authorization request. Each *security message* includes the app identifier (e.g., application name and identity mark) and a text message specifying the ongoing operation and the set of sensitive device sensors being accessed.

Preventing Misuse of Privacy-Sensitive Sensors

Protection

- Laboratory-Based User Study (90 Subjects)
- Users avoided mistakenly authorizing unwanted operations 96% of the time on average, compared to 20% on average when using first-use or install-time authorizations

Usability

- Field-Based User Study (24 Subjects - 21 Widely-Used Apps)
- 3 Apps - Same number of explicit authorization
- 18 Apps - Limited number of explicit authorization (at most 9)

Compatibility

- Compatibility Test Suite (1,000 Most-Downloaded Apps)
- Only 3 minor compatibility issues addressed in subsequent prototypes

Performance Overhead

- UI/Application Exerciser (1,000 Most-Downloaded Apps)
- 0.33% system-wide overhead
- Order of tens of microseconds per access (Unnoticeable to Users)
- 3 MB of cache (operation bindings)

Takeaways

PennState

Classic Access Control Models

- Unable to Identify dynamically-created audio channels
- Unable to identify malicious vs benign use of sensed data
- Unable to enforce contextual use of privacy-sensitive sensors

Need of new approaches and mechanisms

- MLS to control/mediate Audio Channels
- Agility maneuvers that leverage synthetic data to achieve uniform distribution of data points
- Operation binding that captures display context to prevent GUI attacks

Thank You
For Your Attention

Giuseppe Petracca
Ph.D. Candidate
gxp18@cse.psu.edu
http://sites.psu.edu/petracca/