



Dispositivi mobile e rischi per la privacy

Un’indagine sperimentale sull’utilizzo occulto del microfono dello smartphone





Delfina Malandrino – Alfonso Guarino

Antonio Junior Citarella

Indice



Analisi del problema



Cosa è stato fatto finora?



Cosa vogliamo fare?

Analisi del problema

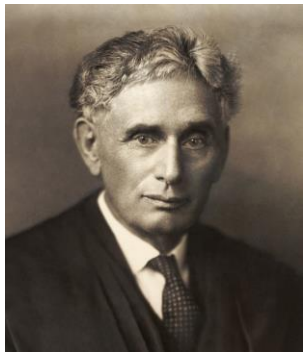
Indice





Analisi del problema

Origini della privacy



Louis Brandeis

Samuel Warren



they argued that technology was creating a new harm.
“Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life,

Nel 1890 pubblicano ‘*the right to privacy*’ introducendo per la prima volta il concetto di riservatezza.
Il right to be alone.

Questo concetto si è poi evoluto nel tempo.
Ai giorni nostri parlare di riservatezza è insensato.
Oggi si preferisce parlare del diritto alla tutela dei propri dati personali.

Analisi del problema

Tipologie di dato

Sono **dati personali** le informazioni che identificano o rendono identificabile, **direttamente o indirettamente**, una persona fisica e che possono fornire informazioni sulle sue caratteristiche, le sue abitudini, il suo stile di vita, le sue relazioni personali, il suo stato di salute, la sua situazione economica, ecc..

i **dati che permettono l'identificazione diretta** - come i dati anagrafici (ad esempio: nome e cognome), le immagini, ecc. - e i **dati che permettono l'identificazione indiretta**, come un numero di identificazione (ad esempio, il codice fiscale, l'indirizzo IP, il numero di targa)

Anche **dati rientranti in particolari categorie** sono dati personali: si tratta dei dati cosiddetti '*sensibili*'.





Analisi del problema

Dati sensibili

I seguenti dati personali sono considerati sensibili e sono soggetti a specifici condizioni di trattamento :

- Dati personali che rivelano la razza o origine etnica, opinione politica, credenze religiose e filosofiche;
- Appartenenza a un sindacato;
- Dati genetici e biometrici utilizzati solitamente per identificare un essere umano;
- Dati sulla salute;
- Dati che riguardano la vita sessuale e l'orientamento sessuale di una persona.

fonte GDPR UE.

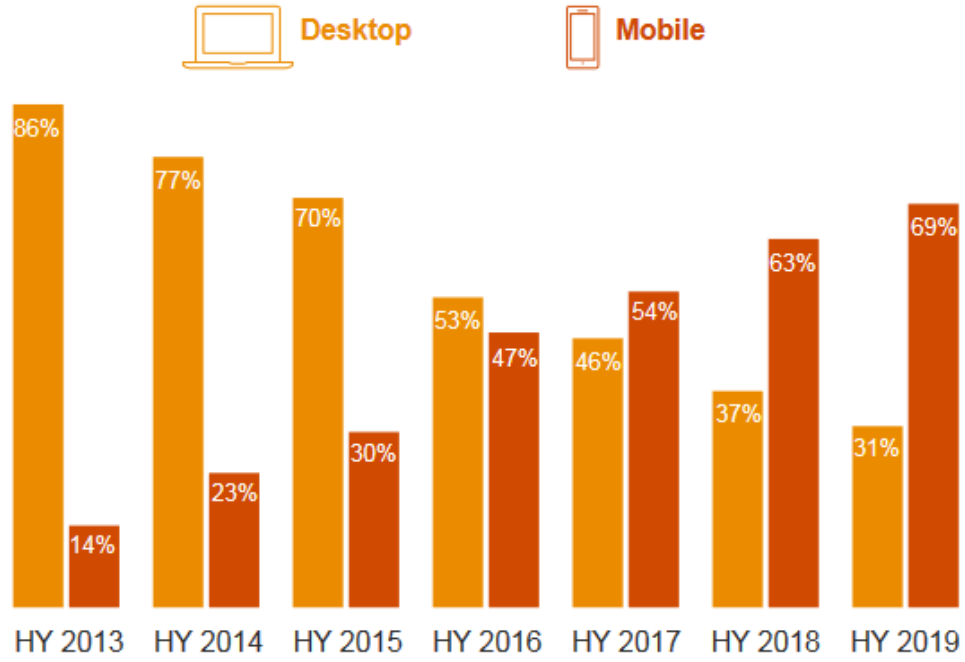
Analisi del problema

Profilazione

La profilazione di un individuo è quindi la costruzione di un **profilo personale** della persona analizzando quelle che sono le sue abitudini e gli interessi, attraverso i suoi dati.

Questa attività era effettuata fino a pochi anni fa solo su dispositivi desktop.

Con l'avvento degli smartphone e delle app che vengono utilizzate su di esso i ricavi che derivano dall'online advertising sono aumentati vertiginosamente.



Source: IAB/PwC Internet Ad Revenue Report, HY 2019

Analisi del problema

Leakage attraverso la raccolta dei dati

Questo attività di profilazione può portare a leakage di informazioni.

Abbiamo scoperto col tempo infatti che in molti siti avveniva una raccolta di informazioni in maniera trasparente, attraverso i cookie ad esempio.

Lo stesso fenomeno potrebbe avvenire anche sui nostri smartphone.





Analisi del problema

Dati su mobile

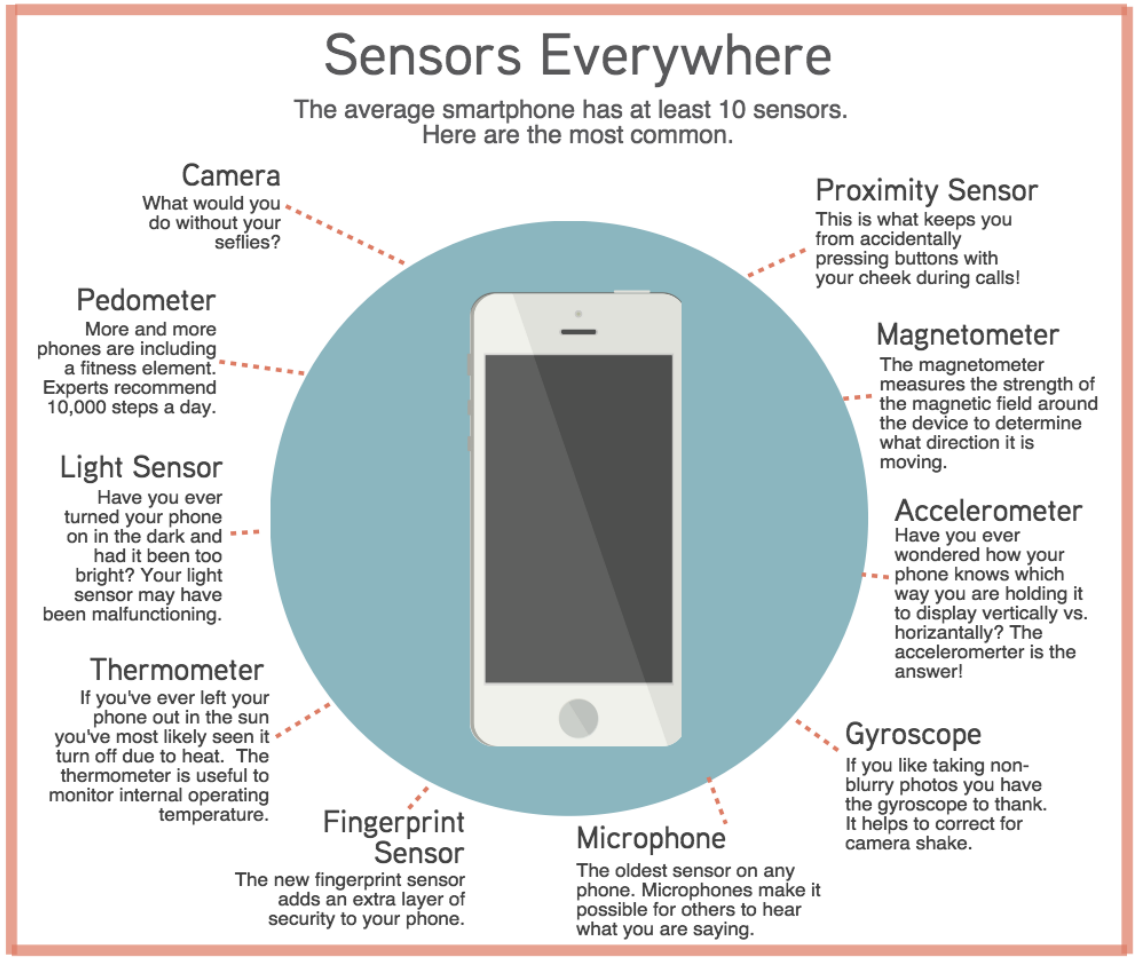
Su piattafome mobile anche il leak di altri tipi di dati potrebbe portare a sgradevoli conseguenze, come ad esempio il numero di telefono

Anche i dati che sono relativi all'hardware dello smartphone, come i sensori, Potrebbero subire un leak.



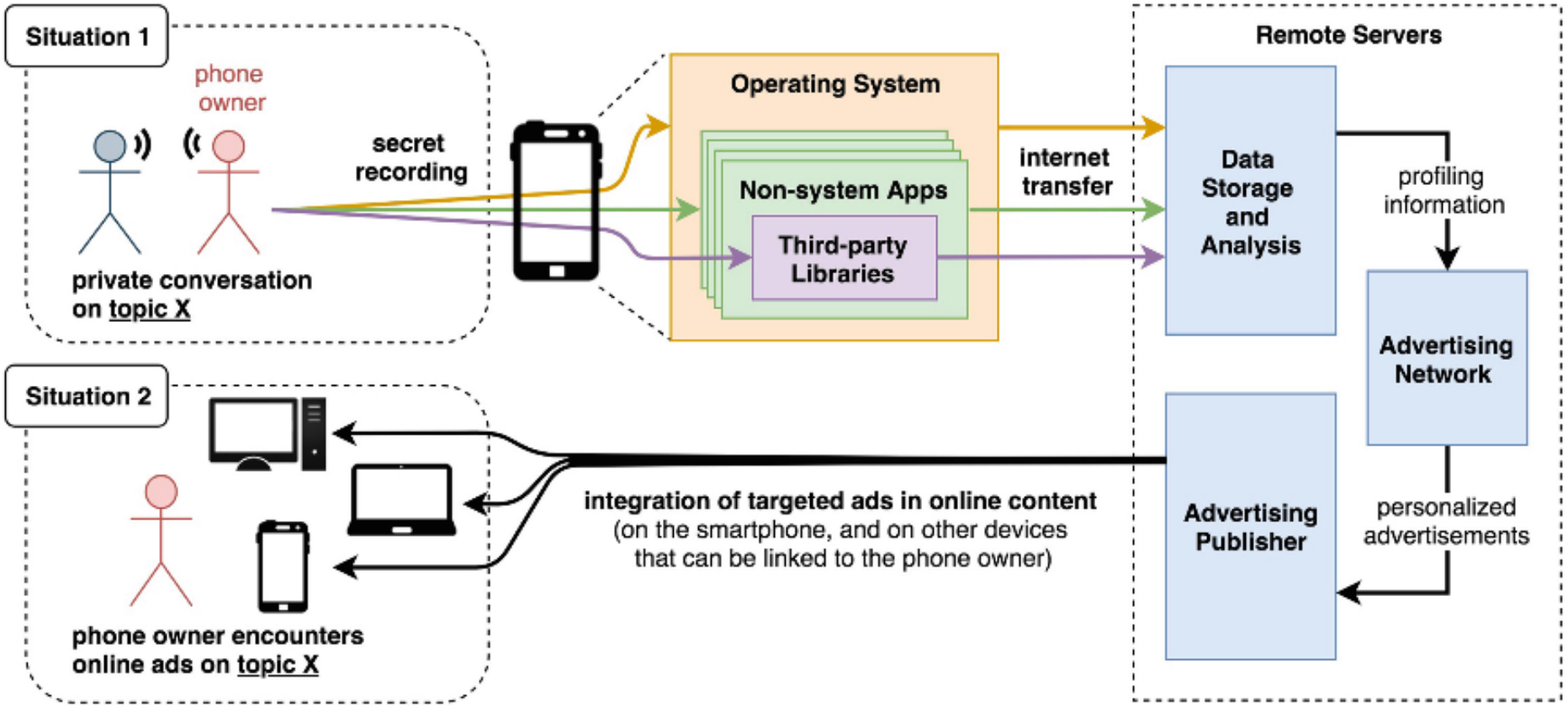


Analisi del problema



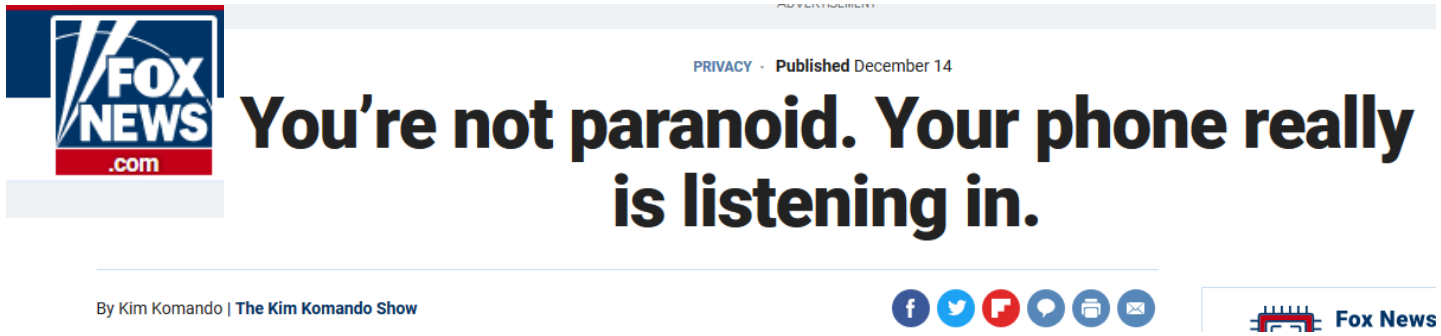
In quali altri modi compagnie di Advertising e di raccolta dati possano prelevare informazioni dai nostri smartphone in maniera trasparente?

Analisi del problema



Analisi del problema

Media popolari parlano di attacchi di intercettazione.

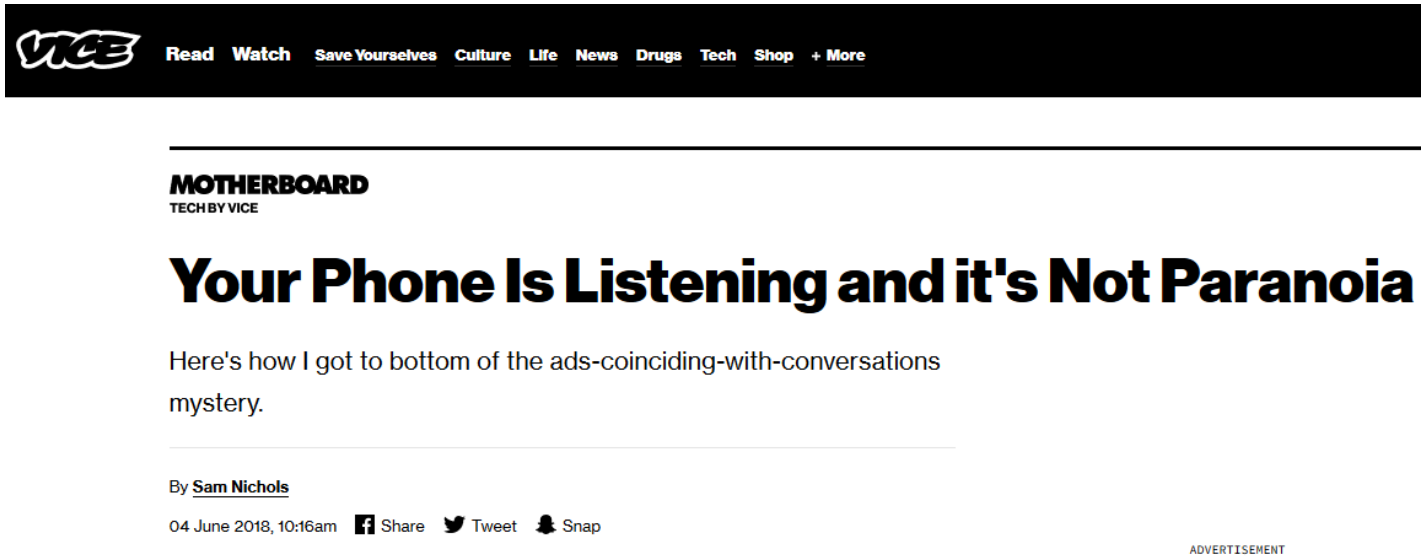


PRIVACY · **Published** December 14

You're not paranoid. Your phone really is listening in.

By Kim Komando | **The Kim Komando Show**

Fox News



VICE Read Watch Save Yourselves Culture Life News Drugs Tech Shop + More

MOTHERBOARD
TECH BY VICE

Your Phone Is Listening and it's Not Paranoia

Here's how I got to bottom of the ads-coinciding-with-conversations mystery.

By **Sam Nichols**

04 June 2018, 10:16am Share Tweet Snap

ADVERTISEMENT

Analisi del problema

Sondaggi effettuati



panda | mediacenter

Survey Findings

We surveyed 1,000 Americans to see if they thought their phone was listening to them.

- 48% of Americans believe that their phone is listening to them.
- In addition, 48% of Americans reported that they have gotten an ad for something they've talked about near a device but never researched online.
- Millennials are more likely to think they are being given an ad for something they haven't ever researched online. Of those aged 18-34, 57% responded that they had experienced this situation while only 37% of those aged 55+ had this occurrence.
- Seniors are less likely to believe their phone is listening to them. Only 36% of those 55+ think that it is.

Forbes

999 views | May 31, 2019, 06:17am EDT

55% Of Americans Say Smartphones Spy On Conversations To Customize Ads



John Koetsier Senior Contributor ⓘ

Consumer Tech

John Koetsier is a journalist, analyst, author, and speaker.

technology gadgets > mobile phones

One in five people think their smartphone is eavesdropping on them

EVER feel you're being watched? Or overheard? You're not alone. Plenty of Aussies are freaked out by targeted social media ads.

news.com.au JULY 19, 2018 12:36AM



Analisi del problema

Regolamentazione relativa al fenomeno.



The Switch

Lawmakers press Apple and Google to explain how they track and listen to users

Top Republican lawmakers on the House Energy and Commerce Committee sent letters Monday asking Apple and Google for more information on how extensively their smartphones track people's locations and record snippets of their conversations.

…In the letters to Google and Apple, lawmakers said the committee is "reviewing the business practices that may impact the privacy expectations of Americans."

Analisi del problema

Regolamentazione relativa al fenomeno.

Bloomberg

Technology

Facebook's Listening Stirs Senator's Ire Over Zuckerberg Remarks

By Ben Brody and Sarah Frier
August 15, 2019, 2:19 AM GMT+2 *Updated on August 15, 2019, 5:52 PM GMT+2*

Democratic Senator Gary Peters of Michigan cast doubt about Mark Zuckerberg's congressional testimony amid revelations that Facebook Inc. has been paying contractors to transcribe audio clips from its users.

…"Congress needs to pass tough rules that ensure that Americans don't have our privacy repeatedly violated by unaccountable corporations," Senator Ron Wyden said in a statement.

…the Irish Data Protection Commission, which oversees Facebook in Europe, said it was examining the activity for possible violations of the EU's strict privacy rules.

Analisi del problema

Le grandi compagnie IT smentiscono

FACEBOOK

Who We Are

Facebook

Facebook Does Not Use Your Phone's Microphone for Ads or News Feed Stories

June 2, 2016

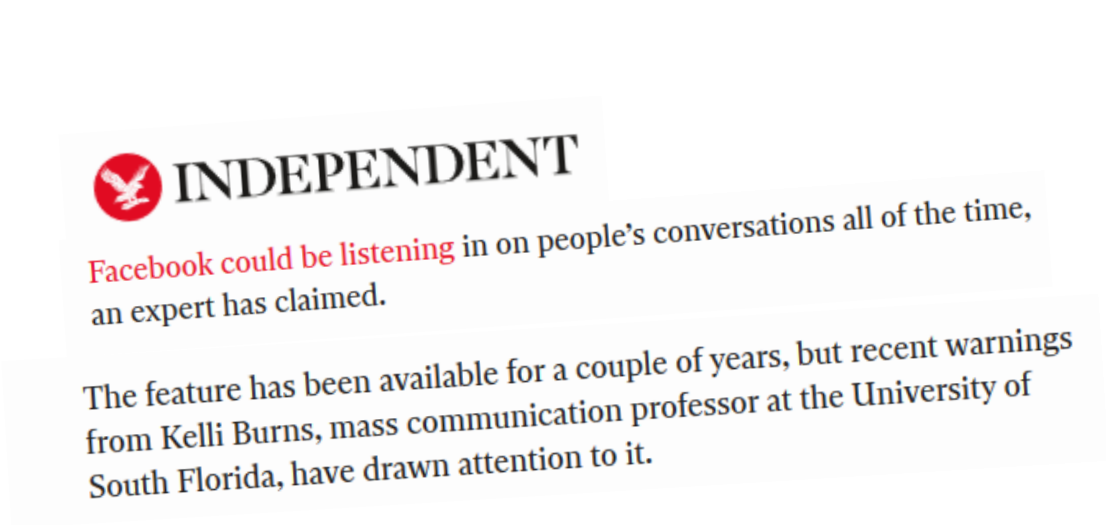
Facebook does not use your phone's microphone to inform ads or to change what you see in News Feed. Some recent articles have suggested that we must be listening to people's conversations in order to show them relevant ads. This is not true. We show ads based on people's interests and other profile information – not what you're talking out loud about.

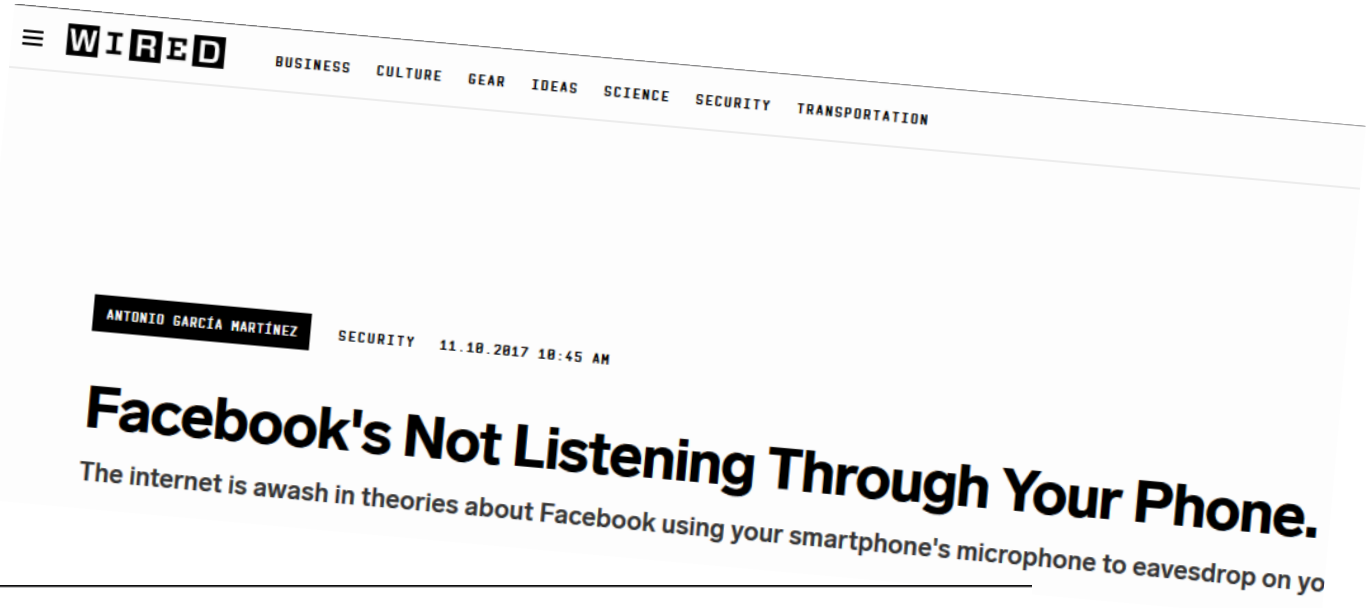




Analisi del problema

Opinioni contrastanti.







Indice



Cosa è stato fatto finora?

Cosa è stato fatto finora?

Ascolto realizzato attraverso sensori di movimento

malintenzionati potrebbero essere in grado di intercettare conversazioni tramite smartphone senza l'utilizzo del microfono.

I sensori di movimento - più precisamente accelerometri e giroscopi - possono essere abbastanza sensibili per captare le vibrazioni del suono e persino ricostruire segnali vocali.

- S Abhishek Anand, Nitesh Saxena. '*Speechless: Analyzing the Threat to Speech Privacy from Smartphone Motion Sensors'.* 2018 IEEE Symposium on Security and Privacy
- Michalevsky, Y., et al.: '*Gyrophone: recognizing speech from gyroscope signals'*. In: Proceedings of the 23rd USENIX Security Symposium. 2013.
- L. Zhang, P. H. Pathak, M. Wu, Y. Zhao, and P. Mohapatral, '*Accelword: Energy efficient hotword detection through accelerometer'.* In Proceedings of the 13th Annual International Conference on Mobile Systems, Applications, and Services. 2015.

Cosa è stato fatto finora?

Ascolto realizzato attraverso sensori di movimento

La possibilità di trasformare i sensori di movimento in microfoni in grado di registrare il parlato ha implicazioni molto significative.

Importante è che l'accesso ai sensori di movimento sugli smartphone, per entrambi i sistemi operativi, è illimitato





- S Abhishek Anand, Nitesh Saxena. '*Speechless: Analyzing the Threat to Speech Privacy from Smartphone Motion Sensors'.* 2018 IEEE Symposium on Security and Privacy

Cosa è stato fatto finora?

Ascolto realizzato attraverso sensori di movimento

Si è analizzato la possibilità di intercettare audio proveniente da una macchina: come ad esempio gli speaker di un laptop.

Chiave degli esperimenti per quanto riguarda l'intercettazione di audio proveniente da una macchina è la necessità che i due dispositivi condividano la superficie di appoggio.

Si è provveduto ad effettuare la sperimentazione sia su una superficie in legno sia su una superficie in plastica.





- S Abhishek Anand, Nitesh Saxena. '*Speechless: Analyzing the Threat to Speech Privacy from Smartphone Motion Sensors'.* 2018 IEEE Symposium on Security and Privacy

Cosa è stato fatto finora?

Ascolto realizzato attraverso sensori di movimento

La frequenza per il parlato è compresa tra 100Hz e 400Hz.

La frequenza per un discorso maschile si trova nell'intervallo 85Hz-180Hz e per una donna da 165Hz-255Hz.

La frequenza di campionamento (indicata anche come velocità dei dati di uscita) comunemente utilizzata dai sensori di movimento è 8kHz per il giroscopio e 4kHz per l'accelerometro

Limite di campionamento implementato nel codice del driver del dispositivo. 200Hz per la piattaforma Android al fine di impedire il consumo della batteria da aggiornamenti frequenti.

- S Abhishek Anand, Nitesh Saxena. '*Speechless: Analyzing the Threat to Speech Privacy from Smartphone Motion Sensors'.* 2018 IEEE Symposium on Security and Privacy

Cosa è stato fatto finora?

Ascolto realizzato attraverso sensori di movimento

Il teorema di campionamento di Nyquist afferma che per acquisire tutte le informazioni sul segnale, la frequenza di campionamento dovrebbe essere almeno il **doppio** della frequenza più alta contenuta nel segnale.

Per i sensori di movimento integrati negli smartphone, la frequenza di campionamento è limitata a 200Hz, il che implica che possono catturare solo frequenze fino a 100Hz.

Pertanto, il sensore di movimento potrebbe essere in grado di catturare solo una piccola gamma del parlato umano nell'intervallo di frequenza **inferiore a 100Hz.**





- S Abhishek Anand, Nitesh Saxena. '*Speechless: Analyzing the Threat to Speech Privacy from Smartphone Motion Sensors'.* 2018 IEEE Symposium on Security and Privacy

Cosa è stato fatto finora?

Ascolto realizzato attraverso sensori di movimento

Si è provveduto ad effettuare un analisi del loro stato sia in una situazione di quiete tramite un analisi del dominio della frequenza e del dominio del tempo.

Si sono ripetute queste analisi con una fonte di segnale sonoro nelle loro vicinanze utilizzando diverse modalità:

- Loudspeaker-Same-Surfer
- Loudspeaker-Different-Surfer
- Laptop-Same-Surfer
- Phone-Different-Surfer
- Human-Normal
- Human-Loud

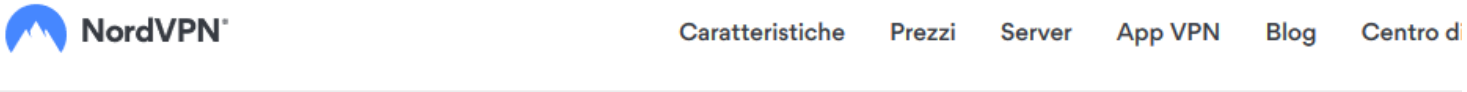
Scenario	Gyroscope affected	Accelerometer affected
Loudspeaker-Same-Surface	*possibly*⋆	✓
Loudspeaker-Different-Surface	×	×
Laptop-Same-Surface	×	*possibly*⋆
Phone-Different-Surface	×	×
Human-Normal	×	×
Human-Loud	×	×

⋆Sophisticated analysis in the frequency domain using machine learning may be able to reveal the impact of speech,

- S Abhishek Anand, Nitesh Saxena. '*Speechless: Analyzing the Threat to Speech Privacy from Smartphone Motion Sensors'.* 2018 IEEE Symposium on Security and Privacy

Cosa è stato fatto finora?

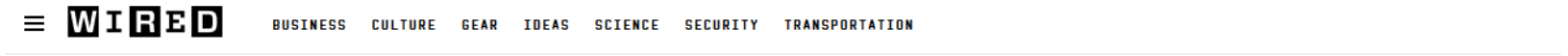
Ultrasonic Beacons



Blog / In Depth /

Ultrasonic beacons: A silent threat to your privacy

May 15, 2017 · 4 min read



LILY HAY NEWMAN SECURITY 04.17.2018 04:15 PM

Ultrasonic Signals Are the Wild West of Wireless Tech

Inaudible signals that your phone can hear—but you can't—are often based on ad hoc tech, which makes for risky security.

Cosa è stato fatto finora?

Ultrasonic Beacons

…ultrasonic beacons are sounds with frequencies from 18 kHz to 20 kHz. Humans can’t hear it, but most mobile devices’ microphones can easily detect the ultrasonic beacons. When emitting from retail stores or embedded to advertisements and even websites, these inaudible sounds are picked up by microphones of mobile devices.





- *Privacy Threats through Ultrasonic Side Channels on Mobile Devices.* Daniel Arp, Erwin Quiring, Christian Wressnegger and Konrad Rieck. 2017. IEEE European Symposium on Security and Privacy (EuroS&P)

Cosa è stato fatto finora?

Ultrasonic Beacons

I ricercatori hanno individuato il codice presente nell'applicazione Silverpush che si occupa di gestire questa tecnica e hanno verificato che altre 234 app, almeno tra quelle prese in considerazione nella ricerca, all'interno dello Store presentano lo stesso codice per l'utilizzo degli ultrasonic beacons.

Tra alcune di queste applicazioni possiamo trovare app di giganti del mercato di fast food come Krispy Kreme e McDonald, le cui versioni Filippine delle app sono presenti nell'elenco.





- *Privacy Threats through Ultrasonic Side Channels on Mobile Devices.* Daniel Arp, Erwin Quiring, Christian Wressnegger and Konrad Rieck. 2017. IEEE European Symposium on Security and Privacy (EuroS&P)

Cosa è stato fatto finora?

Articoli interessanti in letteratura



Is My Phone Listening in? On the Feasibility and Detectability of Mobile Eavesdropping

Jacob Leon Kröger[1,2(✉)] and Philip Raschke[1]

[1] Technische Universität Berlin, Berlin, Germany
{kroeger, philip.raschke}@tu-berlin.de
[2] Weizenbaum Institute for the Networked Society, Berlin, Germany

Dynamic privacy leakage analysis of Android third-party libraries

Yongzhong He[a], Xuejun Yang[b], Binghui Hu[b], Wei Wang[a,b,*]

[a] Beijing Key Laboratory of Security and Privacy in Intelligent Transportation, Beijing Jiaotong University, Beijing 100044, China
[b] School of Computer and Information Technology, Beijing Jiaotong University, Beijing 100044, China

ARTICLE INFO

Article history:
Available online 28 March 2019

Keywords:
Privacy leakage
Third-party library
Android Apps

- *Dynamic privacy leakage analysis of Android third-party libraries.* IEEE Symposium on Security and privacy. 2018. Yongzhong He Xuejun Yang, Binghui Hu, Wei Wang – Beijing Jiaotong University
- *Is My Phone Listening in? On the Feasibility and Detectability of Mobile Eavesdropping.* 33rd Annual IFIP WG 11.3 Conference, DBSec. 2019. Jacob Leon Kröger, Philip Raschke1 -Technische Universität Berlin, Berlin, Germany

Cosa è stato fatto finora?

Articoli interessanti in letteratura



- Valutazione API sensibili utilizzate da app nello store Android
- Sviluppo di un tool che permettesse l'analisi dinamica dei leak di dati sensibili
- Analisi dei dati sensibili che hanno subito un leakage.





- *Dynamic privacy leakage analysis of Android third-party libraries.* IEEE Symposium on Security and privacy. 2018. Yongzhong He Xuejun Yang, Binghui Hu, Wei Wang – Beijing Jiaotong University

Cosa è stato fatto finora?

Articoli interessanti in letteratura

- API sensibili valutate.

Privacy type	System class	Method
IMEI	android.telephony.TelephonyManager	getDeviceId
IMSI	android.telephony.TelephonyManager	getSubscriberId
ICCID	android.telephony.TelephonyManager	getSimSerialNumber
Contact	android.provider.ContactsContract	PhoneLookup
Phone Number	android.telephony.TelephonyManager	getLine1Number
SMS	android.telephony.SmsManager	sendTextMessage
MIC	android.media.MediaRecorder	getAudioSource
MIC	android.media.MediaRecorder	startRecording
Camera	android.hardware.Camera	setPreviewDisplay
Sensors	android.hardware.SensorManager	getDefaultSensor
GPS Location	android.location.LocationManager	getLastKnownLocation
GPS Location	android.location.LocationManager	requestLocationUpdates
GPS Location	android.location.LocationManager	getLongitude
Cell Location	android.telephony.TelephonyManager	getCellLocation

- *Dynamic privacy leakage analysis of Android third-party libraries.* IEEE Symposium on Security and privacy. 2018. Yongzhong He Xuejun Yang, Binghui Hu, Wei Wang – Beijing Jiaotong University

Cosa è stato fatto finora?

Articoli interessanti in letteratura

- API sensibili valutate.

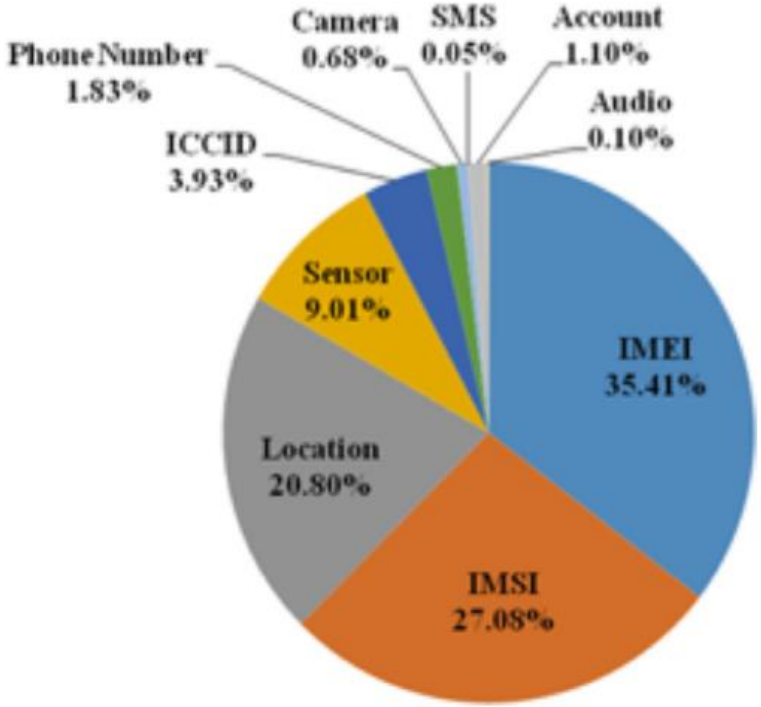
Privacy type	System class	Method
IMEI	android.telephony.TelephonyManager	getDeviceId
IMSI	android.telephony.TelephonyManager	getSubscriberId
ICCID	android.telephony.TelephonyManager	getSimSerialNumber
Contact	android.provider.ContactsContract	PhoneLookup
Phone Number	android.telephony.TelephonyManager	getLine1Number
SMS	android.telephony.SmsManager	sendTextMessage
MIC	android.media.MediaRecorder	getAudioSource
MIC	android.media.MediaRecorder	startRecording
Camera	android.hardware.Camera	setPreviewDisplay
Sensors	android.hardware.SensorManager	getDefaultSensor
GPS Location	android.location.LocationManager	getLastKnownLocation
GPS Location	android.location.LocationManager	requestLocationUpdates
GPS Location	android.location.LocationManager	getLongitude
Cell Location	android.telephony.TelephonyManager	getCellLocation

- *Dynamic privacy leakage analysis of Android third-party libraries.* IEEE Symposium on Security and privacy. 2018. Yongzhong He Xuejun Yang, Binghui Hu, Wei Wang – Beijing Jiaotong University

Cosa è stato fatto finora?

Articoli interessanti in letteratura

- Percentuale leak dati sensibili.



- *Dynamic privacy leakage analysis of Android third-party libraries.* IEEE Symposium on Security and privacy. 2018. Yongzhong He Xuejun Yang, Binghui Hu, Wei Wang – Beijing Jiaotong University

Cosa è stato fatto finora?

Articoli interessanti in letteratura

- In che modo potrebbe avvenire l'intercettazione
- Tecniche esistenti per la scoperta di app potenzialmente ostili sugli store
- Come l'ecosistema possa essere potenzialmente l'attaccante.
- Analisi su come si possano superare le difficoltà computazionali ed economiche





- *Is My Phone Listening in? On the Feasibility and Detectability of Mobile Eavesdropping.* 33rd Annual IFIP WG 11.3 Conference, DBSec. 2019. Jacob Leon Kröger, Philip Raschke1 -Technische Universität Berlin, Berlin, Germany

Cosa è stato fatto finora?

Articoli interessanti in letteratura

- In che modo potrebbe avvenire l'intercettazione:

Per accedere al microfono, le app hanno bisogno del permesso dell'utente. Una ricerca [*] recente ha evidenziato come su 308 utenti Android, solo il 17% di questi prestava attenzione ai permessi.

L'intercettazione potrebbe poi avvenire, come già detto, attraverso l'utilizzo dei sensori di movimento

[*] *Android Permissions: User Attention, Comprehension, and Behavior.* : SOUPS '12: Proceedings of the Eighth Symposium on Usable Privacy and Security. 2012.
Adrienne Porter Felt, Elizabeth Ha, Serge Egelman, Ariel Haney, Erika Chin, David Wagner



- *Is My Phone Listening in? On the Feasibility and Detectability of Mobile Eavesdropping.* 33rd Annual IFIP WG 11.3 Conference, DBSec. 2019. Jacob Leon Kröger, Philip Raschke1 -Technische Universität Berlin, Berlin, Germany

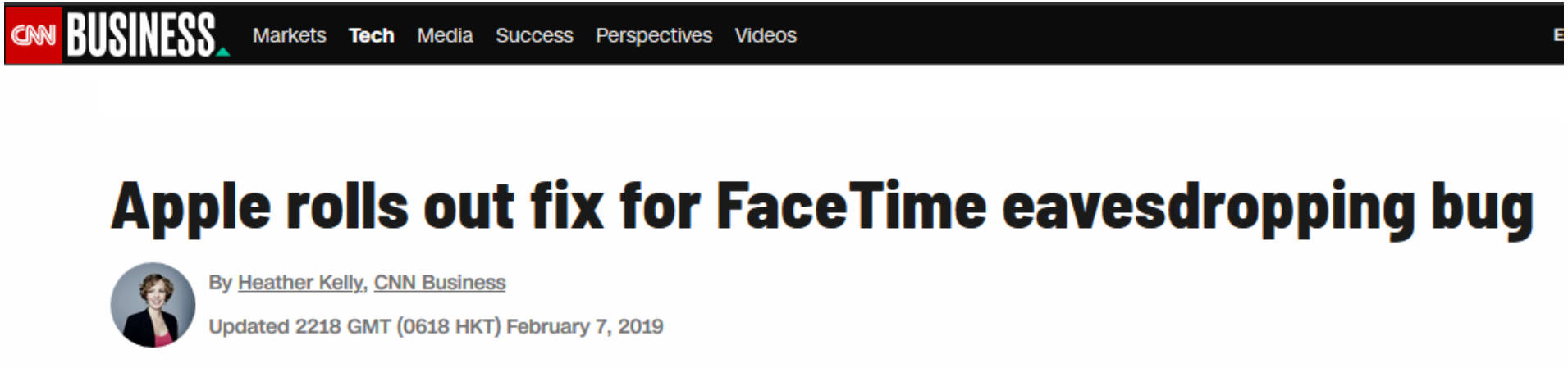


Cosa è stato fatto finora?

Articoli interessanti in letteratura

- Tecniche esistenti per la scoperta di app potenzialmente ostili sugli store:
- Come l'ecosistema possa essere potenzialmente l'attaccante:

Apple e Google effettuano analisi per prevenire l'installazione sui dispositivi di applicazioni potenzialmente pericolose. Tuttavia, innumerevoli esempi di malware inizialmente non rilevati e perdite di privacy hanno dimostrato che non sempre ci riescono



- *Is My Phone Listening in? On the Feasibility and Detectability of Mobile Eavesdropping.* 33rd Annual IFIP WG 11.3 Conference, DBSec. 2019. Jacob Leon Kröger, Philip Raschke1 -Technische Universität Berlin, Berlin, Germany

Cosa è stato fatto finora?

Articoli interessanti in letteratura

- Come ridurre la potenza computazionale ed economica richiesta:

  Registrazione audio di **bassa qualità**.

  Pre-elaborazione locale.

  Rilevamento **parole chiave** invece di riconoscimento vocale completo.

  Registrazione selettiva.

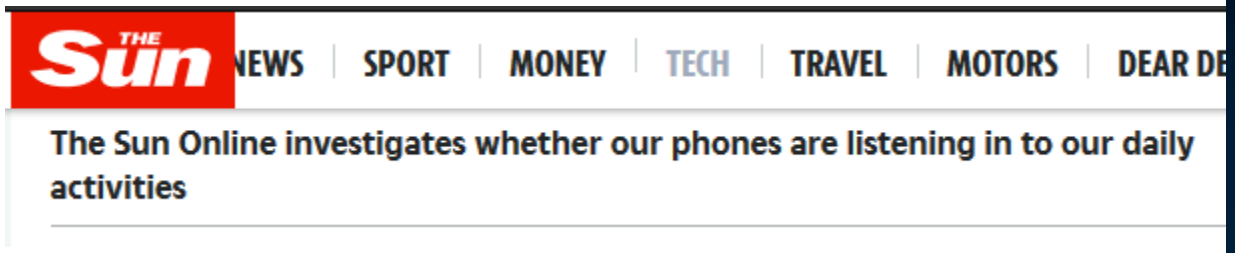




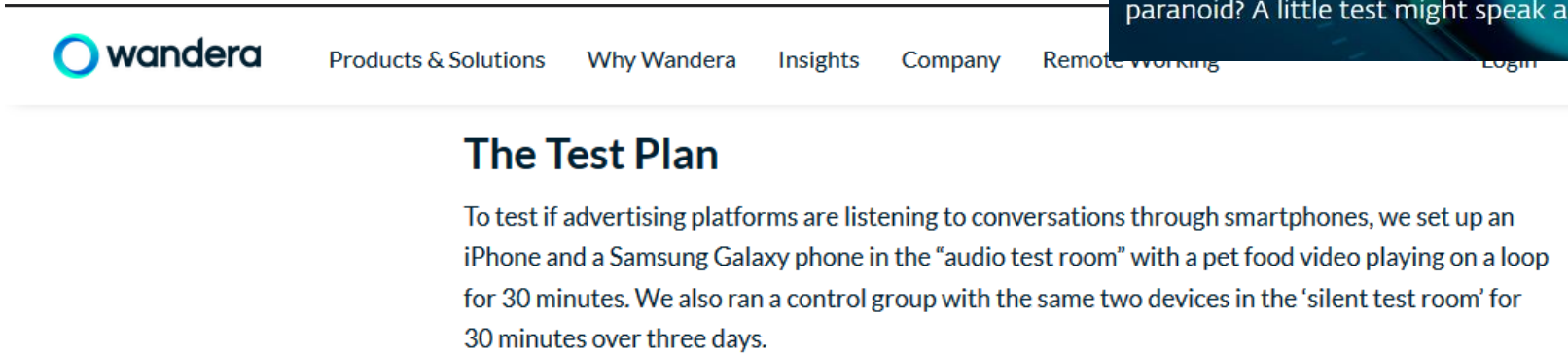
- *Is My Phone Listening in? On the Feasibility and Detectability of Mobile Eavesdropping.* 33rd Annual IFIP WG 11.3 Conference, DBSec. 2019. Jacob Leon Kröger, Philip Raschke1 -Technische Universität Berlin, Berlin, Germany

Cosa è stato fatto finora?

Esperimenti condotti comunità online







Indice





Cosa vogliamo fare?



Cosa vogliamo fare

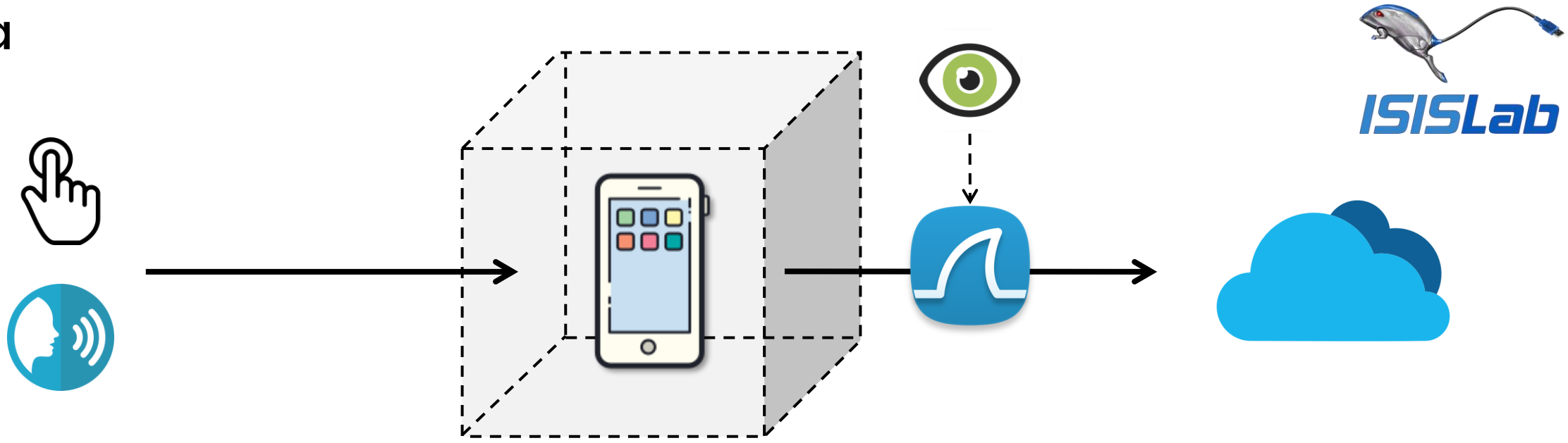
Riassumendo

- Abbiamo visto che tramite i nostri dispositivi mobile avviene un leakage dei nostri dati
- La possibilità che avvenga un intercettazione delle nostre conversazioni per attività di profilazione c'è
- Vogliamo studiare sperimentalmente ed empiricamente questo fenomeno





Idea



Method



Phase 0:
Configuration

Phase 1:
Interaction

Phase 2:
Check Ads

Phase 3:
Traffic Analysis







Grazie per l'attenzione



