Unconventional Mechanisms for Biometric Data Acquisition via Side-Channels

Dr Jonathan Francis Roscoe
Dr Max Smith-Creasey

Our Hypothesis

Devices intended for non-biometric purposes may contain **sensing capabilities from which biometrics can in fact be derived** without a user's knowledge. Such unconventional biometric acquisition methods may be implemented by a hacker wishing to steal biometric information. It is therefore important to discuss how such biometrics could be obtained in order to attempt attack mitigation.

Conventional Biometrics

- Conventional biometrics are considered those that are collected from sensors placed for the intended purpose of biometric collection. For example...
  - Fingerprints from fingerprint scanners on mobiles
  - Facial information from cameras for mobile device unlock

- Conventional biometric acquisition mechanisms are the most widely used type of biometric collection techniques and have begun to replace PINs/passwords. This makes biometrics a valuable resource.

- Unconventional biometric acquisition mechanisms are defined as those that are collected from sensing capabilities that are not intended for biometric data collection.

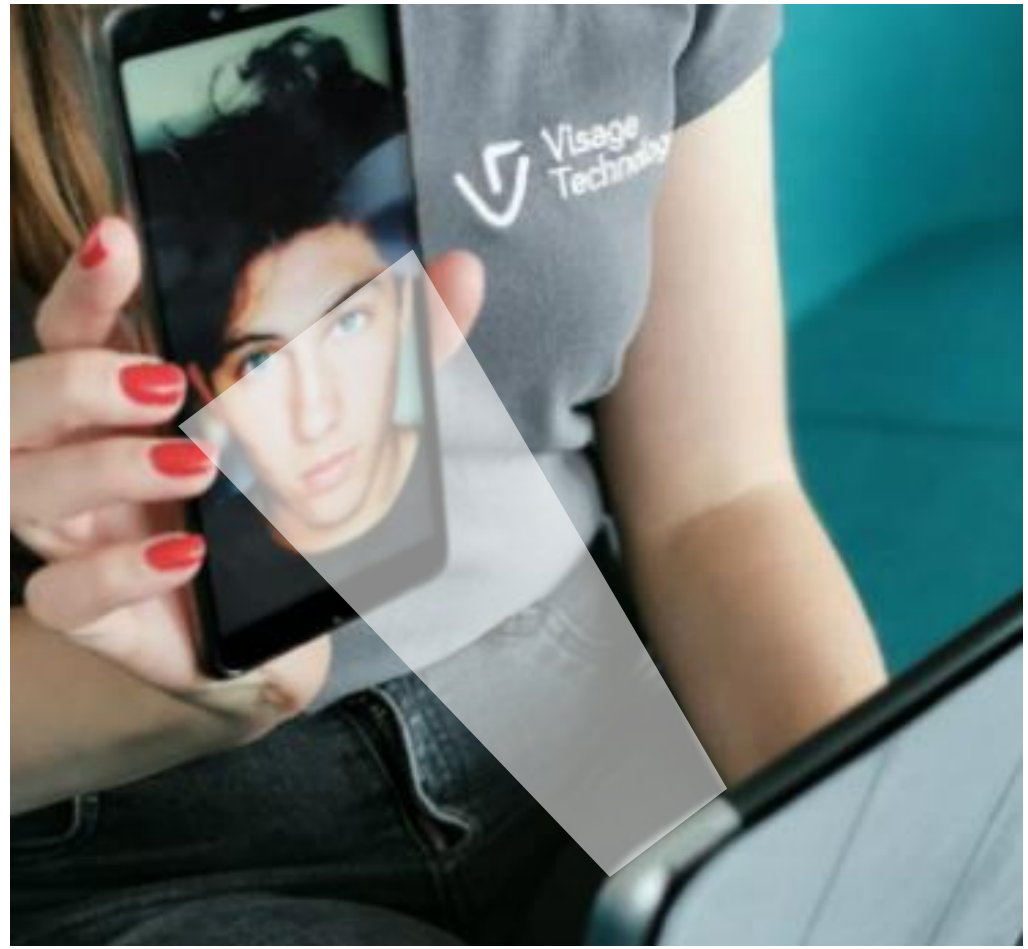
- This presents a security risk to systems using conventional biometrics because an attacker may obtain the user's biometrics via unconventional means.

Security and Privacy Concerns of Biometrics

- Capturing a user's biometrics poses both a privacy risk and a security risk.

- Biometrics can be used to tell information about a user they may wish to keep private (such as personal behaviours/habits).

- Furthermore, the security risk of replay/spoofing attacks from biometrics captured by an attacker presents a very real security risk. For example, on mobile devices successful attacks have spoofed fingerprints and faces.

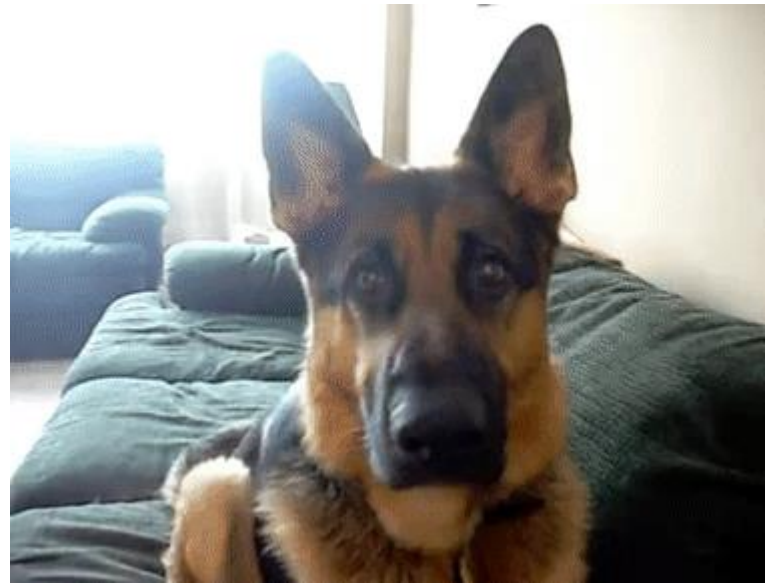


via: https://visagetechnologies.com/face-anti-spoofing-face-recognition/

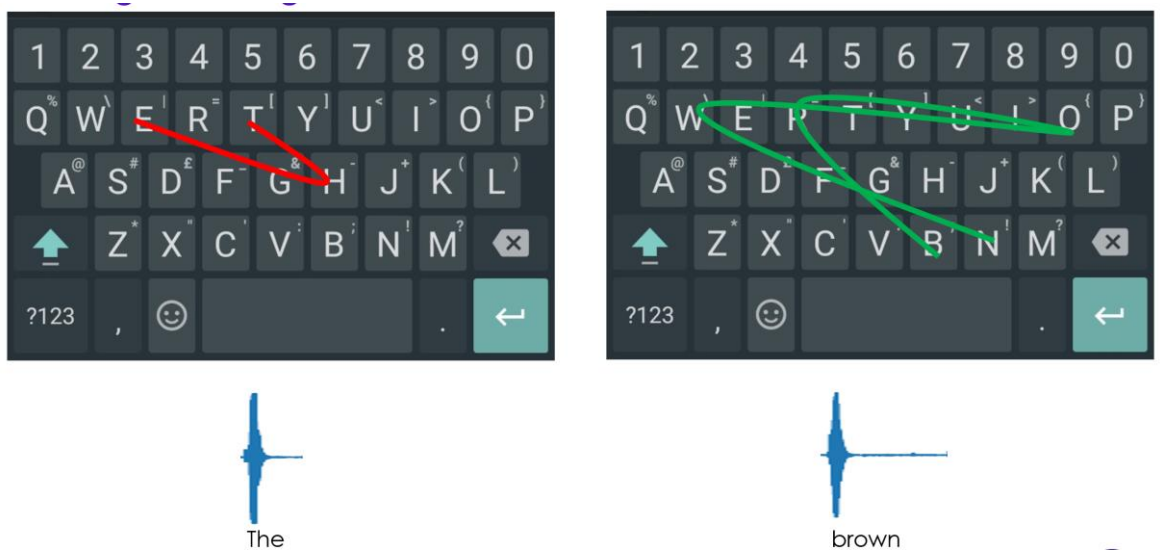
Side-Channels

Non-conventional attack channels that occur due to the way in which a system is implemented.

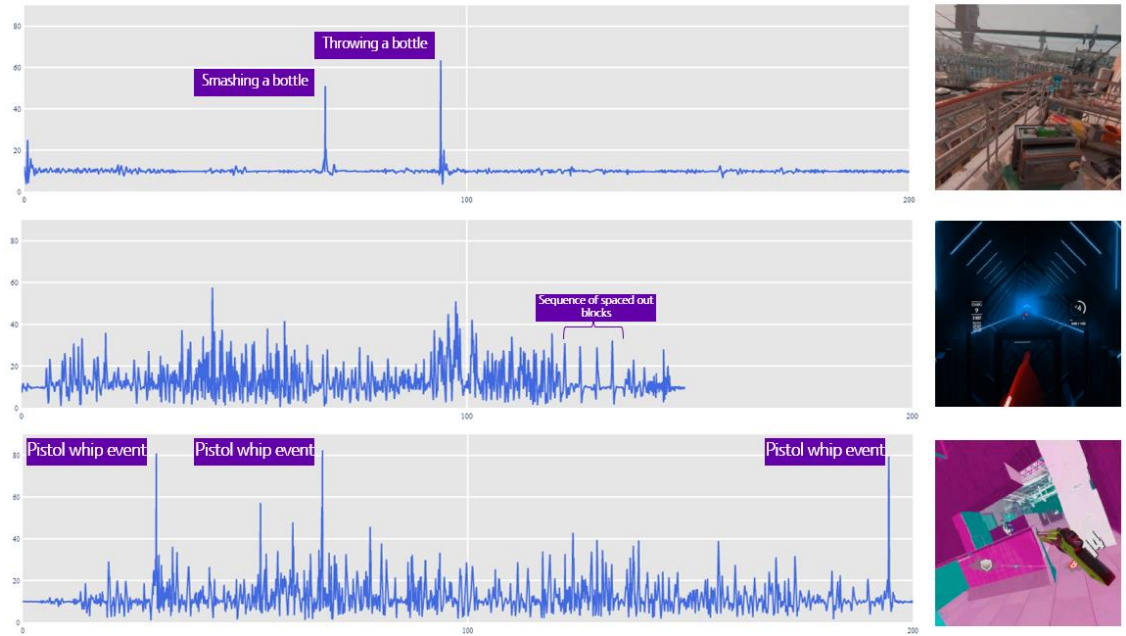
- Timing
- Acoustic emanation
- Thermal properties
- Electromagnetic radiation
- Optical emission
- Power usage
- Fault analysis



Our Previous Research

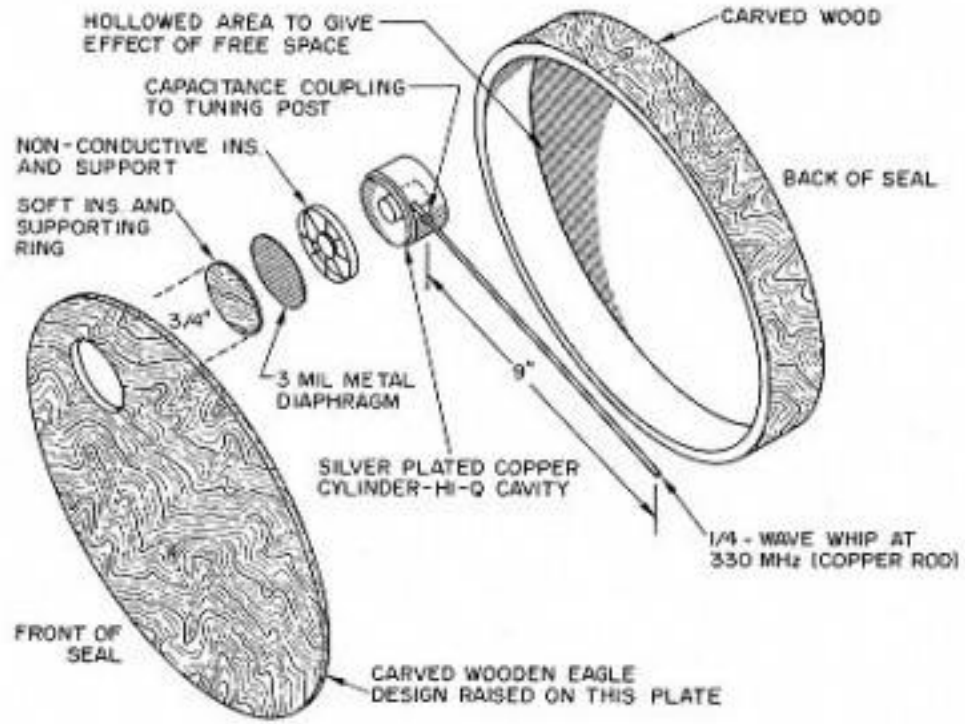


J. F. Roscoe and M. Smith-Creasey, "Acoustic Emanation of Haptics as a Side-Channel for Gesture-Typing Attacks", International Conference on Cyber Security and Protection of Digital Services (Cyber Security), IEEE, 2020



T. Andrade, M. Smith-Creasey and J. F. Roscoe, "Discerning User Activity in Extended Reality Through Side-Channel Accelerometer Observations", International Conference on Intelligence and Security Informatics (ISI), IEEE, 2020

Feasibility of Attack

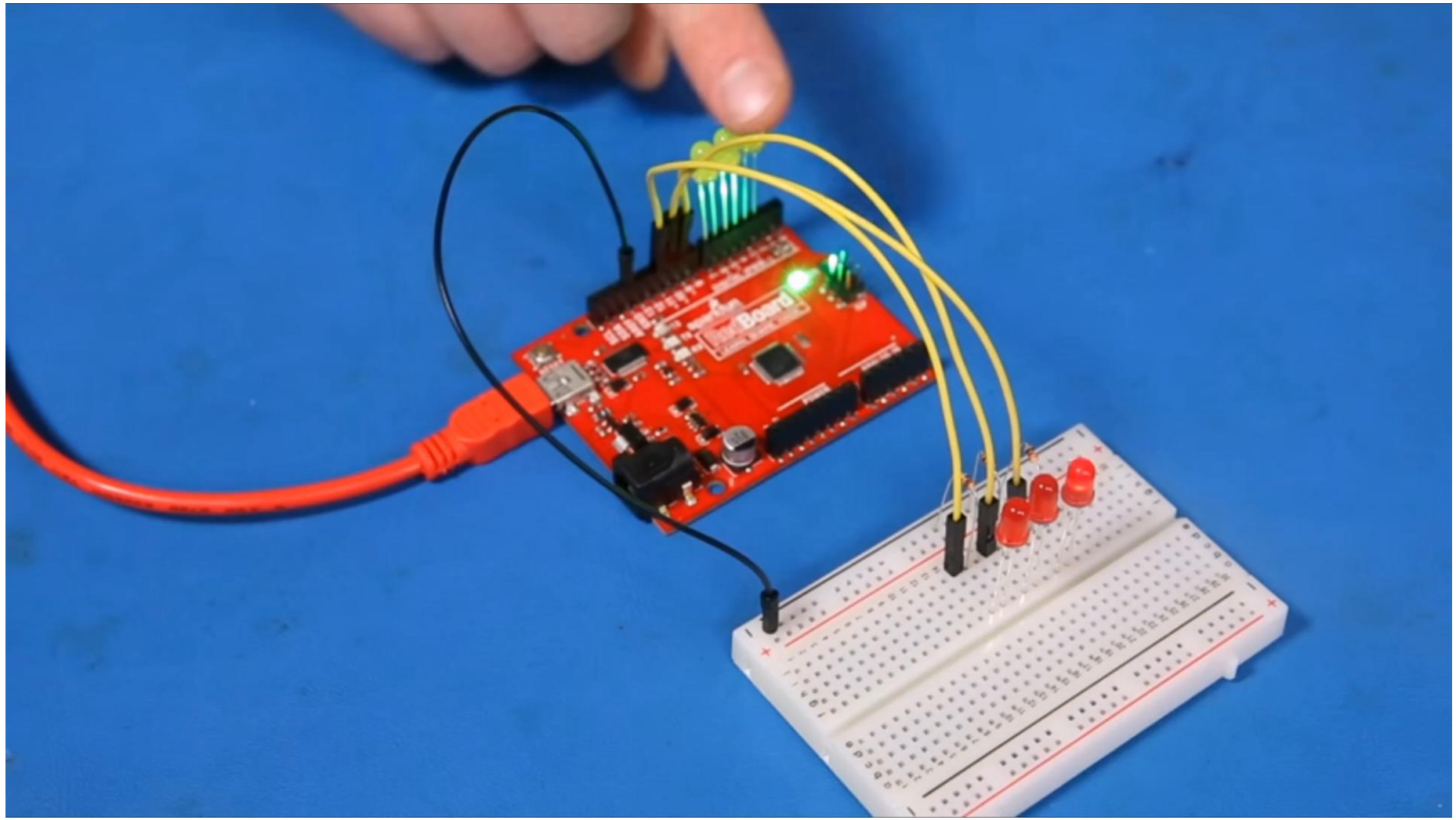


Theremin's "great seal bug" given to US ambassador in Moscow, a 1940s passive eavesdropping device.

Feasibility of Attack

There's no shortage of smart devices with a variety of sensors and connectivity.

Hardware Hacking Examples



LEDs used as sensors. Source: https://www.sparkfun.com/news/2161

Collecting Biometrics in Unexpected Ways

Developing a Low Cost Capacitive ECG via Arduino and Single Board Computer Interfaced with Capacitive Electrodes for Prevention and Security Aspects

J. Güttler and T. Bock

Chair of Building Realization and Robotics,
Technical University of Munich, Germany
E-mail: joerg.guettler@br2.ar.tum.de

Biometric Gait Authentication Using Accelerometer Sensor

Davrondzhon Gafurov, Kirsi Helkala, and Torkjel Søndrol
Norwegian Information Security Lab - NISlab
Department of Computer Science and Media Technology
Gjøvik University College
P.O. Box 191, 2802 Gjøvik, NORWAY
{davrondzhon.gafurov, kirsi.helkala}@hig.no, mail@torkjel.com

Using Light Emitting Diode Arrays as Touch-Sensitive Input and Output Devices

Scott E. Hudson
Human-Computer Interaction Institute
Carnegie Mellon University, Pittsburgh, PA 15213
E-Mail: scott.hudson@cs.cmu.edu

Acoustic Emanation of Haptics as a Side-Channel for Gesture-Typing Attacks

Jonathan Francis Roscoe, Max Smith-Creasey
Future Security and Cyber Defence,
BT Applied Research, Adastral Park, UK
{jonathan.roscoe, max.smith-creasey}@bt.com

The Visual Microphone: Passive Recovery of Sound from Video

Abe Davis[1] Michael Rubinstein[2,1] Neal Wadhwa[1] Gautham J. Mysore[3] Frédo Durand[1] William T. Freeman[1]
[1]MIT CSAIL [2]Microsoft Research [3]Adobe Research

We Can Hear You with Wi-Fi!

Guanhua Wang[†], Yongpan Zou[†], Zimu Zhou[†], Kaishun Wu[‡§], Lionel M. Ni[†‡]
[†] Department of Computer Science and Engineering
[‡] Guangzhou HKUST Fok Ying Tung Research Institute
Hong Kong University of Science and Technology
[§] College of Computer Science and Software Engineering, Shenzhen University
{gwangab, yzouad, zzhouad, kwinson, ni}@cse.ust.hk

Hard Drive of Hearing: Disks that Eavesdrop with a Synthesized Microphone

Andrew Kwong[1], Wenyuan Xu[2], and Kevin Fu[1]

[1]University of Michigan spqr.eecs.umich.edu
[2]Zhejiang University usslab.org

Some capabilities are more obvious than others.

Table of Potential Side-Channels for Unconventional Biometric Acquisition

Table 1: Summary of popular components of smart devices and the biometric patterns they might collect.

	Physical							Behavioural				Soft-biometrics
	Fingerprint	Facial	Ear	Eye	Iris	Voice	Heartrate	Keystroke	Gait	Location	Spatial Gesture	
Microphone						x		x			x	x
Camera	x	x	x	x	x			x	x			x
LEDs												x
Radio							x				x	x
Thermometer												x
PIR												x
Accelerometer / Gyroscope									x		x	
Capacitance sensor	x	x										
GPS										x		x
Ambient light sensor												x
Network traffic												x

Summary of sensor capabilities identified in the literature.

Future Work

- Build a full ontology of potential side-channels
- Explore the susceptibility of consumer hardware to remote subversion of hardware behaviour
- Develop a mechanism for consumer awareness of device capabilities (e.g. nutritional facts label)

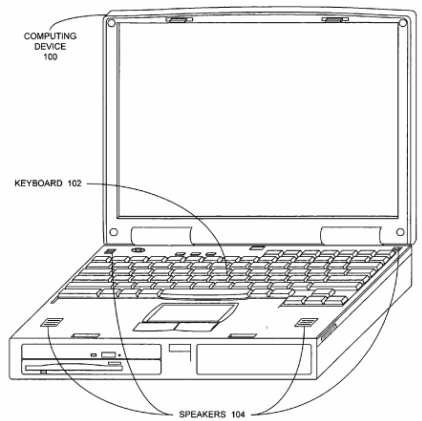
Conclusions

- There are significant overt capabilities in modern consumer devices
- Lack of public awareness
- There exists the opportunity and motivation for eavesdropping via these unconventional channels
- Countermeasures are possible in some circumstances

Patent Application
Tribble et al.

METHOD AND APPARATUS FOR MASKING ACOUSTIC KEYBOARD EMANATIONS

Correspondence Address:
APPLE COMPUTER, INC.



ANC patent for physical keyboards.

Any Questions?

Please get in touch:

jonathan.roscoe@bt.com
max.smith-creasey@bt.com