Unconventional Mechanisms for Biometric Data Acquisition via Side-Channels

Jonathan Francis Roscoe
Security and Cyber Defence
BT Applied Research
Adastral Park, UK
jonathan.roscoe@bt.com

Max Smith-Creasey
Security and Cyber Defence
BT Applied Research
Adastral Park, UK
max.smith-creasey@bt.com

***Abstract*—In this paper, we discuss the proliferation of household smart devices and review the literature to explore whether the implementation characteristics of such systems may provide avenues of attack to obtain private biometric data. Examples include the use of mechanical hard drives as audio microphones and interception of soft-keyboard input through audio analysis of haptic feedback. As the use of biometric data increases in casual environments, the opportunity for it to be stolen in unexpected ways is also increasing. There are many examples of the technology being utilised by hackers to enable unexpected use such as spoofing. We examine the importance and sanctity of biometric data in the modern world and posit that manufacturers must avoid complacency and advocate secure design, to ensure security and privacy of users.**

***Index Terms*—biometrics, iot, smart device, eavesdropping, side-channel, attack**

I. Introduction

The term "biometric" refers to measurements of either physiological or behavioural characteristics of the human body. Measurement and analysis of biometrics has proven useful in a variety of health, security and user experience applications.

Biometric data is data that reflects the physiological/behavioural traits of an individual [1]. Such data is commonly collected with user consent via sensors on a device they are using. The role of this data is often to identify who the user is through matching the biometric traits collected from the sensors to a known biometric profile.

The capability of biometrics to uniquely identify individuals makes it an extremely effective security mechanism. However, it also poses a privacy risk as unlike conventional credentials, they are not easily transferred or replaced. If a biometric such as a fingerprint is obtained by an attacker, they may be able to use this to bypass many systems using this as way of authenticating. Biometrics, particularly behavioural traits, may carry sensitive and private information about an individual that they may not wish to share. This means biometric data is one of the most sensitive and important to protect.

It has been observed that a number of technologies can be utilised to capture biometric data in a previously unintended manner, e.g. in [2] where typing behavhour was used to infer typed sentences. Implementation characteristics that enable such activity are known as "side-channels".

The remainder of this short paper is organised as follows. Section II discusses conventional biometric strategies. Section III discusses the unconventional strategies of collection. Section IV concludes the paper.

II. Conventional Biometrics & Motivation

This section describes the most popular and current biometric techniques. Physiological biometrics are made use of in everyday technologies from smartphones to border control and include traits such as face, fingerprint and iris. Many mobile devices released in 2020 provide the option to use the face or fingerprint to unlock. Conversely, behavioural biometrics are often less overt because they rely on the learning of a user's routine rather than a simple presentation of a physiological trait. Such biometrics include location, movement and environment data and have attracted academic interest [3].

The future trends in biometric systems will see greater use of biometrics to authenticate users. This is because such techniques mitigate the issues with conventional PINs and passwords such as over-the-shoulder attacks and user inconvenience. As more devices include sensors (e.g.: smartwatches) it will also be possible to harness biometric data for both health and authentication purposes. The use of biometrics for authentication motivates the need to identify which biometrics can be considered vulnerable to side-channel collection.

Biometrics can enhance day-to-day life by providing quick authentication, customised services and personalised feedback. However, the discussed uses of biometrics thus far has focused on biometrics that the user is aware of and are not controlled by a malicious user. As discussed, the biometrics collected from a trusted device and a side-channel device implemented by an attacker could be identical and used maliciously for bypassing authentication mechanisms or identity fraud. We call the side-channels "unconventional biometric aquistition" methods and highlight them as privacy issues.

Devices intended for non-biometric purposes may contain sensing capabilties from which biometrics can in fact be derived without a user's knowledge. Such unconventional biometric aquistition 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.

	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

TABLE I
SUMMARY OF POPULAR COMPONENTS OF SMART DEVICES AND THE BIOMETRIC PATTERNS THEY MIGHT COLLECT.

III. UNCONVENTIONAL BIOMETRIC ACQUISITION

In previous work we have demonstrated the ability to eavesdrop on gesture typing input by analysing the time period in audio recordings between haptic feedback events [2], in this case, the audio from haptic actuators was inadvertently revealing the typing pattern of the user. This highlights a key issue, that there are non-obvious approaches to capturing user actions that could yield identifiable biometrics, an ability that can increase in the face of hardware manipulation.

In this section we discuss common electronic components and the opportunity they offer for capturing information beyond their original purpose and the biometrics that may be associated with. Our findings are summarised in Table I. Soft-biometrics are measures such as skin colour, gender and height that do not uniquely identify an individual but may help narrow a search space. A combination of soft biometrics may be suitable for identifying individuals in limited scenarios [4]. It is important to note that many of the examples used are based on laboratory setups and may remain hypothetical in a consumer environment with standard hardware.

Accelerometer data has been similarly used to detect users input [5] on a mobile device and even assess their mood [6]. It can be used to determine the activity of a user and is commonly found in commercial fitness devices [7]. Gait can be captured with accelerometer sensors [8]. It has also been shown that individual accelerometers may have minute variation in manufacturing, making them uniquely identifiable due to variations in response to identical stimuli [9]. With an emerging market for enterprise extended reality devices, it has been demonstrated that monitoring user movement through wearable accelerometers (as found in smart watches, mobile phones, etc.) can be used to identify user activity and effectively eavesdrop on their input [10].

A light emitting diode (LED) is conventionally used as an indicator, component of a display or for environmental lighting. However, when reversed in a circuit, an LED acts as a light sensor [11]. In this state, an LED can thus be used as a single pixel image sensor, suitable for applications such as proximity and presence. Dedicated photodetectors are common components, often used for measuring ambient light, but may also be used in other applications, such as blood flow and heartrate detection (usually combined with LEDs [12], [13].

General purpose image sensors are used for photography and video communication in modern devices, whilst specialist modules may be suitable for iris/retina, fingerprint and facial recognition (as segmentation and matching algorithms rely on quality input) often combined with infrared illumination [14].

Depending on image sensor view and quality, there are a number of biometrics that can be potentially captured from still images or video such as gait [15] as well as soft-biometrics that cannot identifying a particular individual, but significantly reduce search space such as skin or clothing colour. Soft-biometrics can be effectively captured with relatively low quality imaging [16]. Imaging has also been effectively used to reproduce sound by monitoring disturbance in objects in the environment, such as a crisp packet [17]. A conventional smart phone camera is sufficient for detecting heart rate [18].

The use of mechanical hard drives as audio microphones [19], that can reconstruct sound in an environment in a high enough quality for recognition by services such as Shazam [20]. The key enabler of this trick is the small DC motor present in a hard drive to actuate the read/write head. Audio could potentially be used to collect biometric patterns such as typing and voice.

Audio has been demonstrated as a means of achieving non-line-of-sight (NLOS) imaging [21] by bouncing audio signals around corners, potentially making it applicable as a proximity and motion detector.

NLOS has been performed using other parts of the electromagnetic spectrum such as WiFi [22] to visualise the movement and activity of individuals through walls. This has shown to be sufficient to reconstruct mouth movements for a predefined vocabularly [23] enabling reconstruction of speech, though whether speech (in contrast to voice) is sufficient as a biometric remains to be seen. Radio equipment covering very high frequency (VHF) and super high frequency (SHF) bands such as WiFi and Bluetooth are common in connected device. Similar techniques have been used for contact free monitoring of heartrate [24]. Microwave sensors are also commonly used in a similar way to passive infrared (PIR) sensors for presence and proximity detection. Commercial applications of such

technology have been employed to detection hand gestures in 3D space [25].

Capacitance sensing is typically a feature of touchscreen technology and in mobile devices can be used to measure physical biometric patterns such as ear shape and hand proportions [26]. But capacitance sensing comes in many forms and the circuitry to implement rudimentary sensing of capacitance is straightforward and can be done with popular microprocessors [27]. It is also a popular technique for fingerprint sensing [28].

Network traffic from interactive devices such as personal computers, games consoles, etc. can be used to identify users [29]. Device usage can be used to profile users and may even be able to determine mood based on changes in routine behaviour [30].

Other common sensors such as the magnetometer and barometer may be useful as part of an aggregate profile, based on typical subject behaviour and exposures.

IV. Conclusions

We have demonstrated that there exists a potential threat landscape from a variety of devices due to the relatively unknown abilities for hardware components to be repurposed to capture biometric patterns. The collection of user biometrics via these side-channels would present a privacy concern and potentially yield breaches in authentication mechanisms. We present this paper as an opportunity for further research into the feasibilty of such attacks and their mitigation.

In future work we intend to explore the different side-channels and their feasiblity in deriving biometrics. Building on Table I we will define an ontology of biometric side-channels would provide a valuable resource for characterising the threat landscape. We will attempt to use the derived biometrics to spoof a biometric system to establish if there is a risk of such attacks being successfully utilised. Lastly, if the attacks are successful, we will investigate strategies to counteract them (e.g.: though classifying data spoofed via side-channel collection).

References

[1] A. K. Jain, A. A. Ross, and K. Nandakumar, *Introduction to biometrics*. Springer Science & Business Media, 2011.

[2] J. F. Roscoe and M. Smith-Creasey, "Acoustic Emanation of Haptics as a Side-Channel for Gesture-Typing Attacks," in *2020 International Conference on Cyber Security and Protection of Digital Services (Cyber Security)*, 2020, pp. 1–4.

[3] M. Smith-Creasey and M. Rajarajan, "A novel scheme to address the fusion uncertainty in multi-modal continuous authentication schemes on mobile devices," in *2019 International Conference on Biometrics (ICB)*, 2019, pp. 1–8.

[4] A. Dantcheva, C. Velardo, A. D'angelo, and J.-L. Dugelay, "Bag of soft biometrics for person identification," *Multimedia Tools and Applications*, vol. 51, no. 2, pp. 739–777, 2011.

[5] E. Owusu, J. Han, S. Das, A. Perrig, and J. Zhang, "Accessory: password inference using accelerometers on smartphones," in *Proceedings of the Twelfth Workshop on Mobile Computing Systems & Applications*, 2012, pp. 1–6.

[6] E. A. Sağbaş, S. Korukoglu, and S. Balli, "Stress detection via keyboard typing behaviors by using smartphone sensors and machine learning techniques," *Journal of Medical Systems*, vol. 44, no. 4, pp. 1–12, 2020.

[7] D. W. Esliger, J. L. Copeland, J. D. Barnes, and M. S. Tremblay, "Standardizing and optimizing the use of accelerometer data for free-living physical activity monitoring," *Journal of Physical Activity and Health*, vol. 2, no. 3, pp. 366–383, 2005.

[8] D. Gafurov, K. Helkala, and T. Søndrol, "Biometric gait authentication using accelerometer sensor." *JCP*, vol. 1, no. 7, pp. 51–59, 2006.

[9] S. Dey, N. Roy, W. Xu, R. R. Choudhury, and S. Nelakuditi, "Accelprint: Imperfections of accelerometers make smartphones trackable." in *NDSS*. Citeseer, 2014.

[10] T. M. Andrade, M. Smith-Creasey, and J. F. Roscoe, "Discerning User Activity in Extended Reality Through Side-Channel Accelerometer Observations," in *18th Annual IEEE International Conference on Intelligence and Security Informatics*, 2020.

[11] S. E. Hudson, "Using light emitting diode arrays as touch-sensitive input and output devices," in *Proceedings of the 17th annual ACM symposium on User interface software and technology*, 2004, pp. 287–290.

[12] G. Valenti and K. R. Westerterp, "Optical heart rate monitoring module validation study," in *2013 IEEE International Conference on Consumer Electronics (ICCE)*. IEEE, 2013, pp. 195–196.

[13] D. Tordera, B. Peeters, E. Delvitto, S. Shanmugam, J. Maas, J. de Riet, R. Verbeek, R. van de Laar, T. Bel, G. Haas *et al.*, "Vein detection with near-infrared organic photodetectors for biometric authentication," *Journal of the Society for Information Display*, vol. 28, no. 5, pp. 381–391, 2020.

[14] K. W. Bowyer, K. Hollingsworth, and P. J. Flynn, "Image understanding for iris biometrics: A survey," *Computer vision and image understanding*, vol. 110, no. 2, pp. 281–307, 2008.

[15] C. Yang, U. C. Ugbolue, A. Kerr, V. Stankovic, L. Stankovic, B. Carse, K. T. Kaliarntas, and P. J. Rowe, "Autonomous gait event detection with portable single-camera gait kinematics analysis system," *Journal of Sensors*, vol. 2016, 2016.

[16] T. Semertzidis, A. Axenopoulos, P. Karadimos, and P. Daras, "Soft biometrics in low resolution and low quality cctv videos," *7th International Conference on Imaging for Crime Detection and Prevention (ICDP 2016)*, 2016.

[17] A. Davis, M. Rubinstein, N. Wadhwa, G. J. Mysore, F. Durand, and W. T. Freeman, "The visual microphone: Passive recovery of sound from video," *ACM Transactions on Graphics (Proc. SIGGRAPH)*, 2014.

[18] R. Zaman, C. H. Cho, K. Hartmann-Vaccarezza, T. N. Phan, G. Yoon, and J. W. Chong, "Novel fingertip image-based heart rate detection methods for a smartphone," *Sensors*, vol. 17, no. 2, p. 358, 2017.

[19] A. Kwong, W. Xu, and K. Fu, "Hard drive of hearing: Disks that eavesdrop with a synthesized microphone," in *2019 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2019, pp. 905–919.

[20] A. Wang, "The shazam music recognition service," *Communications of the ACM*, vol. 49, no. 8, pp. 44–48, 2006.

[21] D. B. Lindell, G. Wetzstein, and V. Koltun, "Acoustic non-line-of-sight imaging," in *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, 2019, pp. 6780–6789.

[22] M. Zhao, T. Li, M. Abu Alsheikh, Y. Tian, H. Zhao, A. Torralba, and D. Katabi, "Through-wall human pose estimation using radio signals," in *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, 2018, pp. 7356–7365.

[23] G. Wang, Y. Zou, Z. Zhou, K. Wu, and L. M. Ni, "We can hear you with wi-fi!" *IEEE Transactions on Mobile Computing*, vol. 15, no. 11, pp. 2907–2920, 2016.

[24] G. Lu, F. Yang, Y. Tian, X. Jing, and J. Wang, "Contact-free measurement of heart rate variability via a microwave sensor," *Sensors*, vol. 9, no. 12, pp. 9572–9581, 2009.

[25] J. Lien, N. Gillian, M. E. Karagozler, P. Amihood, C. Schwesig, E. Olson, H. Raja, and I. Poupyrev, "Soli: Ubiquitous gesture sensing with millimeter wave radar," *ACM Transactions on Graphics (TOG)*, vol. 35, no. 4, pp. 1–19, 2016.

[26] C. Holz, S. Buthpitiya, and M. Knaust, "Bodyprint: Biometric user identification on mobile devices using the capacitive touchscreen to scan body parts," in *Proceedings of the 33rd annual ACM conference on human factors in computing systems*, 2015, pp. 3011–3014.

[27] J. Güttler and T. Bock, "Developing a low cost capacitive ecg via arduino and single board computer interfaced with capacitive electrodes for prevention and security aspects," in *ISARC. Proceedings of the International Symposium on Automation and Robotics in Construction*, vol. 34. IAARC Publications, 2017.

[28] N. Young, G. Harkin, R. Bunn, D. McCulloch, R. Wilks, and A. Knapp, "Novel fingerprint scanning arrays using polysilicon tft's on glass and

polymer substrates," *IEEE Electron Device Letters*, vol. 18, no. 1, pp. 19–20, 1997.

[29] J. Nowak, M. Korytkowski, R. Nowicki, R. Scherer, and A. Siwocha, "Random forests for profiling computer network users," in *International Conference on Artificial Intelligence and Soft Computing*. Springer, 2018, pp. 734–739.

[30] R. Likamwa, Y. Liu, N. D. Lane, and L. Zhong, "Moodscope: Building a mood sensor from smartphone usage patterns," in *Proceeding of the 11th annual international conference on Mobile systems, applications, and services*, 2013, pp. 389–402.