An Offensive and Defensive Exposition of Wearable Computing

PRAKASH SHRESTHA and NITESH SAXENA, University of Alabama at Birmingham, USA

Wearable computing is rapidly getting deployed in many—commercial, medical, and personal—domains of day-to-day life. Wearable devices appear in various forms, shapes, and sizes and facilitate a wide variety of applications in many domains of life. However, wearables raise unique security and privacy concerns. Wearables also hold the promise to help enhance the existing security, privacy, and safety paradigms in unique ways while preserving the system's usability.

The contribution of this research literature survey is threefold. First, as a background, we identify a wide range of existing as well as upcoming wearable devices and investigate their broad applications. Second, we provide an exposition of the security and privacy of wearable computing, studying dual aspects, that is, both attacks and defenses. Third, we provide a comprehensive study of the potential security, privacy, and safety enhancements to existing systems based on the emergence of wearable technology. Although several research works have emerged exploring different offensive and defensive uses of wearables, there is a lack of a broad and precise literature review systematizing all those security and privacy aspects and the underlying threat models. This research survey also analyzes current and emerging research trends and provides directions for future research.

CCS Concepts: • **General and reference** → **Surveys and overviews**; • **Security and privacy** → **Authentication**; **Privacy-preserving protocols**; *Privacy protections*;

Additional Key Words and Phrases: Wearable computing, security requirements, side-channel analysis and countermeasures

ACM Reference format:
Prakash Shrestha and Nitesh Saxena. 2017. An Offensive and Defensive Exposition of Wearable Computing. *ACM Comput. Surv.* 50, 6, Article 92 (November 2017), 39 pages.
https://doi.org/10.1145/3133837

1 INTRODUCTION

"Wearables," "wearable devices," "wearable technology," and "wearable computing" all refer to the emerging computing paradigm that is incorporated into items of clothing and accessories that can be comfortably worn by the users. Wearable devices are being intensively developed in various forms, shapes, and sizes, including those that are "head worn" (e.g., glasses and headsets), "eye worn" (e.g., contact lenses), "wrist worn" (e.g., watches, bracelets, and wristbands), "feet worn" (e.g., shoes), and "body worn" (e.g., e-textiles and smart fabrics). Smartwatches; fitness trackers like those produced by Fitbit; Google Glass, an augmented reality gadget; and Emotiv headset, a wearable brain-computer interface based on electroencephalography (EEG) technology are some of the examples of already ubiquitous wearable devices. Beyond these, there are upcoming new

Authors' addresses: P. Shrestha and N. Saxena, 115A Campbell Hall, 1300 University Boulevard, Birmingham, AL, 35294; emails: {prakashs, saxena}@uab.edu.

https://doi.org/10.1145/3133837

wearables blooming in the market, such as Google's smart contact lens;[1] Studio Roosegaarde Intimacy 2.0,[2] a smart dress that senses the closeness of a wearer with a bystander; Netatmo JUNE,[3] a device that measures the real-time UV exposure; and GPS Pet Tracker, a wearable for a pet to track its location.

Wearable devices clearly bring immense benefits to society and boast improved quality of life for wearers ranging from virtual interaction in augmented reality (AR) to "fitness data"-inspired healthier lifestyles [92]. However, these devices are not without drawbacks. Being almost constantly attached to the body of the wearer, in contrast to traditional devices, wearables raise unique security and privacy vulnerabilities. One inherent threat is privacy leakage due to the "always on" nature of these devices. For example, many businesses ban Google Glass[4] due to privacy issues as the wearer could potentially be recording video all the time with the device's front-mounted camera, which may compromise the privacy of bystanders. Similarly, wearable devices record different types of data (e.g., sensor readings) that are frequently outsourced elsewhere (mainly to online servers) for real-time analysis. Such data can then be abused by malicious actors and may leak sensitive information regarding the wearer itself. For instance, the sexual activity of some of the Fitbit's users had been exposed due to Fitbit's default settings in the recent past.[5] Another threat pertains to the (typically) unguarded access to wearable devices due to their interface-constrained nature. If a wearable device is lost or misplaced, anyone has access to the information stored on the device, since wearable devices generally store data locally without encryption, PIN protection, or user authentication. Finally, an additional threat raised by wearable devices is their exploitation for illegitimate use due to their inconspicuous nature. For example, wearables may be effectively exploited by students for plagiarism purposes, in both traditional and online settings [105].

While wearables introduce the potential for offensive uses, they also hold the promise to help enhance the existing security, privacy, and safety paradigms in unique ways while preserving the system's usability. One of the innovative enhancements can be seen in the context of authentication. Authenticating users based on their thought, particularly brainwave signal, has now become possible due to technological advancement in wearable headsets equipped with EEG sensors [10, 33]. Similarly, an important de-authentication step, which has been overlooked by common authentication schemes, can be addressed by the use of a wearable bracelet, embedded with motion sensors. With such a wearable bracelet, the user can be continuously yet transparently authenticated to a terminal (or even a website) based on motion sensors' readings [101]. Another enhancement lies in pedestrian safety schemes. For instance, the use of a wearable shoe, embedded with inertial sensors, can enable the detection of the sidewalk-to-street transitions, thereby enabling people to identify the pedestrian risks when they step into the street [76]. In this research survey, we provide a comprehensive study of such wearables' driven security, privacy, and safety enhancements to the existing system.

Survey Contribution: The contribution provided by this research survey is threefold (Figure 1 provides a high-level view):

(1) We identify a wide range of existing as well as upcoming wearable devices and investigate their general applications in various domains, such as medical, sports and fitness, and business operations (Section 2).

[1]Google's Smart Contact Lens – https://goo.gl/AbPJYS.
[2]Studio Roosegaarde Intimacy 2.0 – https://goo.gl/kMG6U0.
[3]Netatmo JUNE – https://goo.gl/9Ah7fH.
[4]Although Google Glass is no longer offered by Google, there are other similar smartglasses, such as Sony SmartEyeGlass, Epson Moverio BT-300, and Vuzix M300, which would suffer from similar issues as the Google Glass.
[5]Fitbit Moves Quickly After Users' Sex Stats Exposed – https://goo.gl/BFzME6.

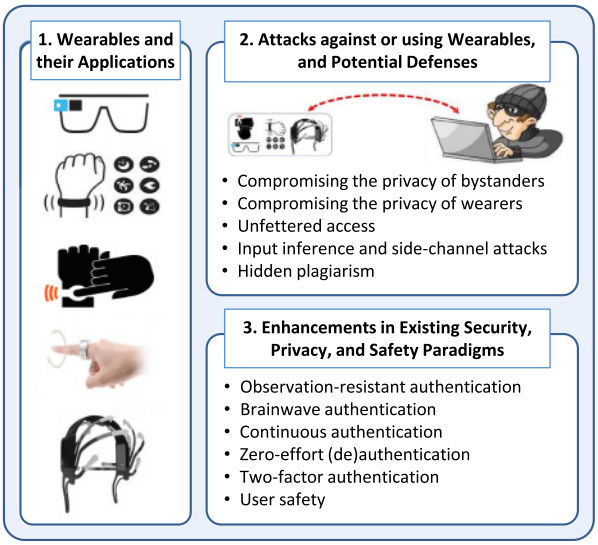

Fig. 1. A high-level overview of the research survey.

(2) We provide an exposition of the security and privacy of wearable computing, studying dual aspects, that is, both attacks as well as defenses (Section 3).
(3) We pursue a comprehensive study of the potential security, privacy, and safety enhancements to existing computing systems based on the emergence of wearable technology (Section 4).

Although several research works have emerged exploring different offensive-defensive uses of wearables, there is still a lack of a broad and precise literature review systematizing all those security and privacy aspects. This research survey analyzes current and emerging research trends and provides directions for future research.

2 WEARABLES AND APPLICATIONS

Wearables enable a number of applications in various domains of life, ranging from personal and medical to business operations.[6] In this section, we explore a variety of wearable devices and provide a brief review of different applications.

(1) *Medical:* In the medical sector, several wearable devices have been introduced to assist medical personnel in monitoring the patient's physiology. Wearables offer simultaneous recording of vital signs, including heart rate, blood pressure, respiration, and body temperature, which contributes to producing a health summary of a patient and an alert message when emergency service is needed. Some wearables, such as QardioCore[7] and Neurosky,[8] also offer remote and continuous monitoring of electrocardiograms (ECG) and EEGs to improve detection and management of cardiac and mental conditions of patients. There exist other wearables that enable clinicians/patients to manage chronic

[6]Wearable Technology Application Chart – http://www.beechamresearch.com/article.aspx?id=20.
[7]QardioCore – https://goo.gl/JWxKM1.
[8]NeuroSky – http://neurosky.com/.

diseases, such as Abbott Diabetes Care,[9] iTBra,[10] and ADAMM.[11] Other wearables, such as *eSight*,[12] *Horus*,[13] *OrCam*,[14] *dbGLOVE*,[15] and *Lechal Shoes or Insoles*,[16] are designed to enhance the vision capability of visually impaired individuals. Some wearables also enhance the hearing capability of a person. Hearing aids from *ReSound*[17] and *Audicus*[18] are some such examples.

(2) *Wellness:* Wearables are being widely used in consumer healthcare with a goal to provide a healthy lifestyle and general well-being. Wearables offer physiological monitoring; emotion monitoring; gait/posture correction; eye and skin care by monitoring UV exposure, humidity, and temperature; identification and assessment of harmful running style; massage and sleep monitoring; and training feedback. *LUMOBack*,[19] *Netatmo JUNE*,[20] *Violet*,[21] and *CliMate*[22] are some such examples.

(3) *Sports and Fitness:* Wearable products offer various applications in the sports and fitness sector, like fitness monitoring, measuring body movement, vibration-based muscle therapy, virtual coaching, and sports performance monitoring and evaluation. Some examples are activity tracker bands (e.g., *Runsense*[23]), fitness sports shoes (e.g., *StretchSense*[24]), and *MYOVOLT*.[25]

(4) *Communications:* Wearable technology features applications related to interaction among people, including text, voice and email, group interaction through social media, and physical expressions such as touch and hugs. Smartwatches, wristbands, smartrings,[26] *smart T-shirt*,[27] and smart undergarments (e.g., Fundawear[28]) are some examples of such wearable products.

(5) *Glamor:* One of the several domains where wearable technology is deployed is the glamor sector, where the general goal is to make a positive impact on appearance and to create fascinating fashion pieces, including decorative displays, light adornments, and tracking displays of emotions on clothing items. Such fashion-centered wearables include light-sensitive dresses, motion-sensitive dresses, stretch-sensitive dresses from Rainbow Winters,[29] and intimacy dresses from Studio Roosegaarde.[30]

[9] Abott – https://www.abbottdiabetescare.com/.
[10] Cyrcadia Health – http://cyrcadiahealth.com/.
[11] ADAMM – http://www.healthcareoriginals.com.
[12] eSight – http://www.esighteyewear.com/.
[13] Horus – http://horus.tech/en/horus.php.
[14] OrCam – http://www.orcam.com/.
[15] dbGLOVE – http://www.dbglove.com.
[16] Lechal – http://lechal.com.
[17] ReSound – http://www.resound.com.
[18] Audicus – https://audicus.com/.
[19] Lumo Back – http://www.lumobodytech.com/lumo-back/.
[20] JUNE – https://www.junebynetatmo.com/en-US/site.
[21] Ultra Violet – http://www.liveultrahealthy.com.
[22] CliMate – https://www.rootilabs.com/products/climate.
[23] Runsense – https://goo.gl/5R9g1u.
[24] StretchSense – http://stretchsense.com/.
[25] MYOVOLT – http://www.myovolt.com/.
[26] DOI SmartRing – https://www.mota.com/doi-smart-ring/.
[27] CUTECIRCUITS – http://cutecircuit.com/tshirtos/.
[28] Fundawear – http://goo.gl/7qxKxJ.
[29] Rainbow Winters – http://www.rainbowwinters.com.
[30] Studio Roosegaarde – https://goo.gl/qqjCGd.

(6) *Business Operations:* The hands-free and location-independent operations of wearables create a number of business applications. A wrist-mounted mini-PC with built-in GPS provides high-tech mobility and connectivity to emergency personnel, search-and-rescue teams, warehouse workers, or anyone on the move [49]. Further, wearables such as *Nymi band,*[31] *NFC Ring,*[32] *Digital Dreams wristbands,*[33] and *MagicBands*[34] offer delivery of better customer service, improved operational efficiency, and access control.

3 SECURITY AND PRIVACY OF WEARABLES

In this section, we first present the security and privacy requirements that need to be considered while designing a wearable computing system. Then, we present a set of security and privacy threats against or of using wearable technologies, in particular an exposition of the state-of-the-art attacks, and potential defenses against those attacks based on the existing research literature.

3.1 Security and Privacy Requirements

There are several security and privacy properties that need to be considered while designing wearable devices and applications. When considering security and privacy properties, usability should also be taken into account. These security, privacy, and usability requirements vis-a-vis wearable computing are listed next.

3.1.1 Security Requirements.

- *Confidentiality*: Only the authorized parties (i.e., an authorized user; an authorized companion device, like a smartphone or PC; or an authorized online server, if any) should be able to access the data recorded by the wearables, the information transferred to/from the wearables, and the system structures of the wearables. These authorized parties should be *verifiable* (i.e., the identity of the wearer or the companion devices communicating with wearables or online server should be authenticated). Specifically, data should remain confidential all along the way from wearables themselves and companion devices to the online services (if any).
- *Integrity*: An unauthorized party should not be able to modify the data recorded by the wearables, the information transferred to/from the wearables, and the system structures of wearables. An adversary should not be able to inject false data or modify or delete the recorded or wearable-relevant information. Further, the adversary should not be able to modify or replace a hardware/software component of the wearable device.
- *Availability*: An authorized party should be able to access the data recorded by the wearables, the information transferred to/from the wearables, and the system structures of wearables when requested. In other words, wearable devices should be resistant against any form of denial-of-service (DoS) attacks. For example, they should be invulnerable against battery-draining attacks, storage-overflowing attacks, or jamming attacks on communication channels.
- *Authentication*: The authenticity of the wearer should be verified using a viable authentication scheme. Only a legitimate owner of the device should be allowed to access the device.

[31]Nymi – https://nymi.com/.
[32]NFC Ring – http://nfcring.com.
[33]Digital Dreams wristbands – http://goo.gl/jsQSAo.
[34]MagicBands – https://goo.gl/kLrPF4.

- *Access Control*: The use of data/information recorded/stored on the wearables should be controlled using access policies. Only a valid user having valid access rights should be allowed to access a particular piece of information associated with a wearable device.
- *Nonrepudiation*: It should be ensured that the wearables cannot deny being the origin of the data that they generated.

3.1.2 Privacy Requirements.

- *Device ID Privacy*: Wearable devices should not be trackable by any unauthorized party. Use of a persistent identifier, such as RFID identifier [79], Bluetooth [77] device address, and 802.11 media access control (MAC) address [63], in clear text can compromise an individual's location. Wearable device IDs should therefore be kept private.
- *Device Log or Measurement Privacy*: The measurements and access log information stored on the device should not be accessible to any unauthorized parties. The malicious entity should not be able to extract any information about the sensitive activity, such as entering a PIN in any POS terminal, a password, or text input on the PC.
- *Wearer Privacy*: An unauthorized party should not be able to exploit the wearable devices to identify the wearer or to learn sensitive information about the wearer. The information may include the name, address, location, audio and video of bearers, and the medical history or detailed diagnosis, in case of a medical device.
- *Bystander Privacy*: A malicious entity should not be able to exploit the wearable devices to identify the bystander or capture/derive sensitive information about the person nearby and in close surroundings. Capturing information about the users' surroundings raises privacy issues toward the social environment as bystanders may not be aware of or compliant with ongoing recordings.

3.1.3 Usability Requirements. Wearables should be able to offer the following fundamental usability features: (1) *easy to put on*—there should not be any tedious steps to set up and install a wearable device on the wearer's body; (2) *easy to keep in position*—once installed/worn, the wearable should remain in its position without any discomfort to the user; and (3) *easy to use*—though limited in physical area for input/output, users should be able to interact with the wearable device easily and comfortably. When considering security and privacy requirements of wearable computing, user experience, particularly the usability features mentioned previously, should also be carefully considered and evaluated. While covering security and privacy requirements of wearables, it may often create a confusing and cumbersome design that causes the user to lose his or her interest and motivation toward wearables. Such a design should be evaluated and avoided if possible. Due to their resource-constrained nature, though designing security and privacy-rich wearable devices creates unique challenges, usability aspects should also be given consideration.

3.2 Threats and Potential Defenses

There are various security and privacy threats against wearable technologies, which are surveyed and systematized next, along with their potential defenses based on existing research literature (Table 1 provides a summary).

3.2.1 Privacy Threats of Wearable Cameras. The wearable "life-logging" cameras (e.g., Google Glass, Autographer, and Narrative Clip) allow users to automatically "life-log" daily activities from the "first person" perspective for various purposes, such as treating memory loss [69]; enhancing public safety, security, and accountability [37] or enjoyment. These cameras capture a large number of images every day, which may include pictures with embarrassing moments or sensitive information (e.g., pictures of computer screens containing private emails or bank account

Table 1. Summary of the Security and Privacy Threats Against or of Using Wearable Technologies, Along with Their Potential Defenses Based on Existing Literature

Threats	Defenses
Privacy Threats of Wearable Cameras	· Design and implementation of Privacy-Enhancing Technologies (PETs)
Unfettered Access	· Design and implementation of on-board secure authentication system leveraging available physiological and motion sensors
Input Inference and Side-Channel Attacks	· Permission restriction to on-board sensors · Privacy-enhancing keyboard · Mitigating acoustic emanations · Mitigating visual leakage of input/output devices · Access control to bio-sensors
Hidden Plagiarisms	· Prohibit the use of wearables in special environments, such as examination scenario · Software-based restriction that prohibits the full usage of device features
Accidental Leakage to Online Services	· Designing wearables capable of working fully offline utilizing hand-held devices · Should give clear and precise information about the data to the user · Minimal personal identification information collection and storage · Encryption of data while storing ("zero knowledge" service)
Hijacking Communication Link	· Use of secure communication protocols
Safety Risks	· Establish clear legal guidelines and policies · Implement software-based mechanisms that automatically identify the risks

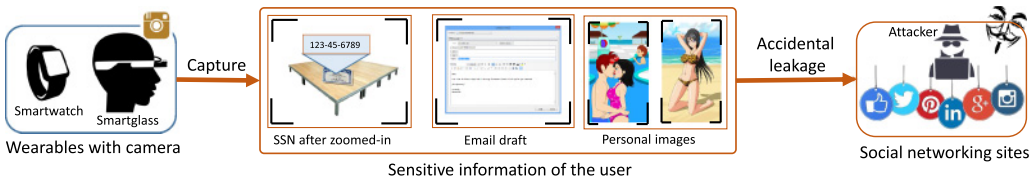

Fig. 2. Some instances depicting privacy threats of wearable cameras.

information) about the wearers and others in the environment that wearers/bystanders may not want to be recorded. Given the massive collection of images captured by the cameras, controlling access to these images becomes a labor-intensive task. Captured images may contain subtle private information. For example, the account information on the captured image may be noticeable only after it is zoomed in. This may cause people to inadvertently share private information, referred to as a "misclosure" [26]. To help people store and share captured images, many wearable devices feature automatic uploading of images to the cloud, which further amplifies privacy concerns. Furthermore, a malicious remote entity can fool the users into installing a visual malware (on their life-logging wearables) that collects the captured images and constructs three-dimensional models of wearers' indoor environments [144]. The malicious entity can then investigate the constructed virtual environment model carefully and steal various virtual objects such as users' whereabouts, personally identifiable information (e.g., SSN), financial documents (e.g., bank account information), and information on computer monitors (e.g., private emails). Such real-time life-logging tools and activities raise a variety of privacy concerns regarding both the bystanders and the wearers.

The hands-free nature and inconspicuous recording abilities of wearable cameras have made capturing and recording images/videos easier than ever. Unlike mobile phones, wearable computers embedded with cameras remain attached to the wearer's body almost all the time. Moreover, these devices are evolving, shrinking in size, and offering low detectability. Unfortunately, these features enable a malicious entity to record the video surreptitiously to get sensitive information about the person or the places of interest. The advancement in computer vision technology has

further enhanced the capability of malicious actors. For instance, a malicious agent can apply various computer vision techniques on a video consisting of a user tapping on the touchscreen to automatically locate the touch points on the screen. Later, by mapping the estimated touch points to a reference image of a standard soft keyboard or number pad of that particular touch-enabled device, the malicious agent can infer the touchstrokes provided by the user [139, 161].

Consequently, life-logging cameras have highlighted the risks of and challenges to the privacy of the bystanders along with that of the wearers. People are interested in being asked permission before being recorded, and wearers are also concerned about the privacy of the bystanders [43, 72, 92]. A few years ago, it was reported in the media that Google Glass users were attacked in public.[35] These media reports underscore the high demand for the design and the implementation of privacy-enhancing policies and techniques geared toward wearable cameras [89].

Potential Defenses: To address the privacy threats pertaining to the use of wearable cameras, a handful of privacy-enhancing policies and techniques, in particular "Privacy-Enhancing Technologies (PETs)," have been proposed in the scientific literature. Some are based on colocation of the camera and its bystanders, while some are based on face recognition. Others require the user to carry some visual markers or perform certain gestures. Table 2 presents a systematization and comparison of different PETs considered in this survey based on the usability, deployability, and security criteria (described briefly in Appendix Table 5) as described in [89]. All these PET approaches can be classified into the following five categories:

(1) *Visual Marker Based:* Visual-marker-based approaches, such as the ones used by *Privacy Makeup* [65], *Respectful Cameras* [130], *Picture Privacy Policy Framework (P3F)* [39], *OfflineTags* [113], and *PrivateEye and WaveOff* [121], track the visual markers using statistical learning and then use various classification techniques to execute respective privacy policies. *Privacy Makeup* and the hairstyle-based approach presented in [65] create significantly invasive distortions with camouflage makeup to prevent the feature response of face detection algorithms. *Respectful Cameras* uses colored hats or vests as the visual marker, while *Offlinetags* uses four different symbols, *No photos*, *Blur me*, *Upload me*, and *Tag me*, which are printable on a piece of paper and readable by the open-source *Offlinetags* software. *P3F* uses similar approaches as *Respectful Cameras*, but the privacy policies used in this scheme are more complex and fine-grained. In addition to dedicated accessories, *P3F* offers a database of fashionable clothing patterns that are used as visual markers. Unlike all these schemes, *PrivateEye and WaveOff* require the user to mark sensitive regions explicitly using a predefined marker or a phone application. *PrivateEye*, intended for privacy of the 2D regions, requires marking of the sensitive region with predefined marker (e.g., dotted rectangle inside the solid rectangle), while *WaveOff*, intended for the privacy of 3D objects, requires marking the sensitive object using the WaveOff phone application. The WaveOff application then extracts and stores the visual features of the sensitive regions in the database to be used later for privacy policy enforcement.

    Thus, the visual-marker-based approach requires the user to wear or carry one or multiple visual markers (e.g., colored vest or hat) to initiate the privacy policy in wearable cameras. Certainly, these visual markers are visible to the bystanders and therefore instantly disclose the users' privacy preferences. Some users may want to reveal their privacy preferences toward recording, while others may not want to do so.

(2) *Location Based:* The privacy preferences of a user can be mediated by certain spaces or locations [43]. For instance, a location such as locker rooms or theaters may require some

[35] Google Glass targeted as symbol by antitech crowd – http://goo.gl/gLikQi.

Table 2. Systematization of PETs Indicating if Certain PETs Satisfy a Given Usability, Deployability, and Security Property

			Usability						Deployability			Security		
Scheme	Reference	Approach/es Used	*User-Initiated*	*Smartphone-Used*	*Dedicated-Device-Required*	*Physical-Artifact-Required*	*Behavioral-Impact*	*Internet-Connection-Required*	*Negligible-Cost-per-User*	*Accessibility*	*Requires-Device-to-Comply*	*Third-Party-Service-Required*	*Anonymity*	*Visibility*
PED Cloak	Brassil et al. (2005)	2		X				X		X	X	X		
BlindSpot	Patel et al. (2009)	2, 5			X					X			X	X
Respectful Cameras	Schiff et al. (2009)	1				X				X	X		X	X
Privacy Makeup	Harvey (2010)	1					X						X	X
Privacy Gesture	Barhm et al. (2011)	4	X								X		X	X
Privacy Visor	Yamada et al. (2012, 2013)	5			X					X			X	X
P3F	Dabrowski et al. (2013)	1				X			X		X			
SnapMe	Henne et al. (2013)	2, 3		X				X	X		X	X		
FaceBlock	Yus et al. (2014)	3		X				X	X		X	X		
Offlinetags	Pallas et al. (2014)	1				X	X			X	X		X	X
PlaceAvoider	Templeman et al. (2014)	2							X	X	X		X	
Do Not Share	Ashok et al. (2014)	5			X					X	X		X	
PriFir	Wu et al. (2015)	6		X					X	X			X	
I-Pic	Aditya et al. (2016)	5, 3			X			X		X	X	X	X	
PrivateEye and WaveOff	Raval et al. (2016)	1	X	X			X		X		X		X	X
TagMeNot	TagMeNot.info (2016)	7				X				X	X		X	X
Cardea	Shu et al. (2016)	2, 3	X	X				X	X		X	X		X

"X" represents the presence of that particular property.

special treatment. As many of the wearable computing devices incorporate GPS sensors, location-based approaches such as *SnapMe* privacy watchdog [68] and *BlindSpot* [115] are feasible to mediate privacy preferences. These approaches are based on the correlation between the location information of the camera and that of the bystanders on the captured images. In addition to location reference, *SnapMe* integrates facial recognition to identify individuals in the pictures. Unlike *SnapMe*, the *BlindSpot* approach first detects the presence of the camera and then directs a pulsing light at the lens of the camera, thereby distorting any imagery that the camera records. Specifically, *BlindSpot* is intended for the fixed camera (e.g., CCTV-like surveillance systems), and thus its area of operation is limited to a specific location. Another prominent location-based approach is *PlaceAvoider* [143], which intends to protect the privacy of bystanders as well as that of the wearer of a wearable camera. Similar to *SnapMe*, *PlaceAvoider* features the blacklisting of privacy-sensitive locations like bathrooms, bedrooms, and meeting rooms. *PED Cloak* [22],

on the other hand, periodically captures and timestamps the users' location coordinates through a PED device (may be a phone) and stores them in the clearinghouse. The clearinghouse also receives the user's preferences toward recording through the PED device. The surveiller or video owner, before publishing the video or image, queries and retrieves the privacy preferences of the person on the video or images from the clearinghouse and executes them accordingly.

The location dependency or location tracking may be a limiting factor of this approach because most users may wish that their devices do not keep track of their locations. The privacy approach should work regardless of specific locations. Moreover, it requires the transmission of location information to the third-party server or nearby device (although over a secure channel), which may create an additional privacy challenge.

(3) *Face Recognition Based:* Face detection and face recognition technology can itself be used creatively to enhance privacy policies. Several schemes, such as *SnapMe* [68], *FaceBlock* [162], *Cardea* [138], and *I-Pic* [2], use this approach, where a user shares privacy preferences along with his or her identity to identify his or her photo in the image captured by a nearby wearable camera. When the wearable camera takes a picture, the system detects and recognizes the faces presented in the picture, checks the policies it has received, and obscures the faces as necessary. All these systems provide a mobile app where the user can configure privacy settings. In addition to facial features, *SnapMe* and *Cardea* also employ location information of the user in the picture to identify the context during a photo shoot. However, this approach also requires the transmission of privacy-sensitive data (user identity and facial image) to the third-party service and therefore creates the additional challenges to preserve the user's privacy.

(4) *Gesture Based:* Gesture is another feasible approach to mediate privacy preferences toward the wearable camera. In *Privacy Gesture* [16], the authors proposed a gesture-based approach that requires a user to perform some predefined gesture to mediate the privacy preferences. However, this approach is limited to the videos containing multiple image frames because it is hard to perform gesture recognition based on a single image frame. Moreover, this approach requires the user to be aware of being recorded, which may not be feasible with most wearable cameras that are usually inconspicuous and undetectable.

(5) *Signal Emission Based:* Specialized devices generating a certain spectrum of light that is transparent to the user but can jam the camera capture could be used in a PET scheme. The work of Yamada et al. [158] proposed *Privacy Visor*, a face-worn device embedded with an infrared light source that obscures the image captured by most of the camera sensors by emitting the infrared signal. Unlike *Privacy Visor*, *Do not share* [11] leverages the infrared signal to transmit the privacy preferences of the user in the form of IR bits to the camera taking a photo or video. The algorithm implemented in the camera or smartphone decodes the received IR signal and executes the preferences as needed. Though the infrared signal is invisible to the human eye and makes it a suitable option for regulating privacy policies, the notion of using it as a medium is expensive as it requires a dedicated device. Another disadvantage of this approach is that the user needs to carry a specialized device all the time, which may not be feasible in all scenarios (e.g., at a beach).

(6) *Sensor Based:* A multitude of sensors, including an accelerometer, gyroscope, or light sensor, available in ubiquitous devices, such as smartphones and smartwatches, can be used to detect the sensitive environment around the user. With the sensitivity of the environment derived from the sensors' data, privacy preferences of the user can be regulated on wearable cameras. The work in *PriFir* [154] has shown that the low-power sensors on smart devices can be used to generate the fingerprint of sensitive scenarios, such as typing,

visiting the restroom, or indoor versus outdoor, and later utilized to mediate the privacy preferences of the user.

(7) *QR-Code Based:* Privacy preferences of the user can be encoded in the form of the QR-code. Whenever such QR-code is detected on an image/video, the privacy policy as obtained by decoding such QR-code can be executed accordingly. *TagMeNot* [27] leverages a similar approach; that is, the user carries a QR-code corresponding to his or her privacy preferences, and the image/video recording application on the wearable device decodes it and executes the appropriate privacy policy.

Beyond the privacy issues with images/videos captured by wearable cameras, these devices have recently raised another privacy issue: *display leakage on transparent near-eye displays*. Transparent displays, in contrast to a normal wearable camera, allow the device's user to see the information shown on the display as well as the outside of the display (i.e., see the world) simultaneously. However, recent research at Microsoft Research [85] has found display leakage in multiple near-eye displays: *Google Glass, Silicon Micro Display ST-1080, Meta One, and Lumus*. By observing a user wearing the transparent near-eye display, an adversary can recreate the display contents from the light leaked through the "outward-facing" unit of the display. The key reason behind this leakage is the design flaw in the display system, specifically due to *"the transparent and symmetrical nature of the display system"* [85].

The use of "Polarization" and "Narrowband Illumination" can be potential defenses against such near-eye display leakage [85]. Ambient light and display light have different polarization and can be separated by polarization. Through the use of an appropriate polarizer, the display light of one polarization can be restrained within the display. Another defense is through the use of narrowband (i.e., laser) illumination of a Liquid Crystal on Silicon (LCoS) microdisplay. The use of a narrowband filter would prevent the display light from being seen or reflected.

3.2.2 Unfettered Access. In practice, most of the wearable devices generally do not offer the authentication functionality, and even if the wearables offer a built-in authentication scheme, it is not convenient, and therefore users would be hesitant to use it. Often, such authentication is not established directly between the user and the wearable, but rather indirectly through the companion smartphone or PC. The lack of methods to authenticate the wearables is partly perhaps because these devices became widely available recently, and also because such devices have a small form factor and are typically constrained in terms of input/output interfaces, battery power, and computational and storage capabilities. As a result, traditional authentication schemes designed for resource-rich devices (e.g., smartphones or PCs) cannot be directly applied in the context of wearables. Wearables, many being personal devices, contain sensitive and personal information about the wearer. For instance, wearable devices may contain login information of social media or bank account information. Due to the absence of an authentication mechanism, authorized access to the data recorded by the wearables is therefore not guaranteed, raising the serious potential for abuse by a malicious agent.

Potential Defenses: A simple approach to defending against unfettered access to wearable devices is to implement an on-board secure authentication mechanism. However, as these devices usually do not possess a keyboard or sometimes even a touchscreen, they introduce challenges in implementing traditional password-based authentication schemes on such devices. These devices also create new opportunities to implement secure authentication schemes as they usually embed a variety of physiological and motion sensors. For instance, wearable devices are emerging with various bio-sensors, like those capturing heart signals (ECG), muscle signals (EMG), and brain signals (EEG), and motion sensors, like accelerometers and gyroscopes. By utilizing the signals

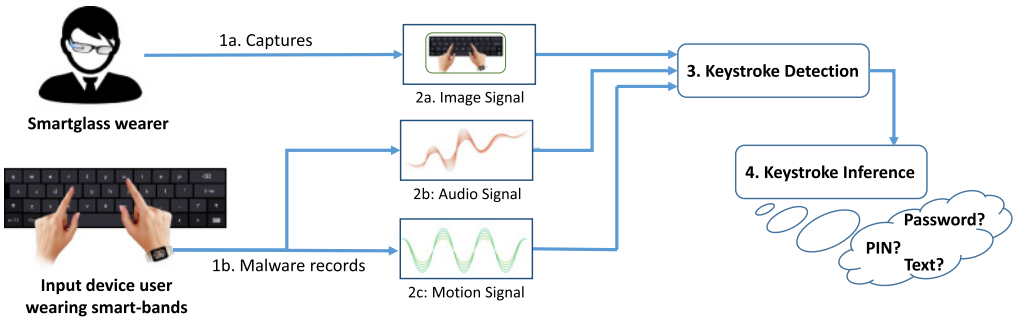

Fig. 3. High-level overview of input inference and side-channel attacks. Malicious app/entity can utilize the image, audio, or motion signals captured through the wearable device (smartglass, or smartwatch) to launch a side-channel input inference attack.

captured by these sensors, various authentication schemes can be designed that are both secure and usable.

Several authentication mechanisms have been proposed for authenticating a user to wearable glasses, such as the Google Glass. *"Bulletproof"* is the first and oldest authentication scheme, which was released in April 2013 [44]. *"Screen Lock"* is another authentication scheme developed by Google [62]. Both of these schemes are gesture-based authentication schemes that unlock the device based on a user's gesture pattern on the glass touchpad. Later, Yadav et al. Yadav et al. [157] proposed two novel PIN-based authentication schemes: *"Touch-based PIN (TBP)"* and *"Voice-based PIN (VBP),"* where the user enters or utters a cipher PIN derived from the actual PIN in a wearable headset. Chan et al. [29] proposed "*Glass OTP*," a One-Time-Password (OTP)-based authentication scheme. In *Glass OTP*, a glass camera is used to scan a QR code (encoding one-time password), which is displayed on the user's phone. Schneegass et al. Schneegass et al. [132] proposed a novel biometric authentication scheme, *"SkullConductm,"* that uses frequency characteristics of the audio signal as it travels through the head of the user. The research conducted in [127] proposed an in-air hand-gesture-based authentication scheme, "*VSig*." We discuss and evaluate all these authentication approaches (in terms of their usability, deployability, and security) later in Section 4.1.

The approaches mentioned may not be feasible for implementation on wearable devices other than the head-worn devices. So, for such devices, new authentication schemes should be explored. For example, the Nymi wristband [108] uses heart rhythm or fingerprint biometrics to authenticate the wearers to the device. A similar approach can be applied to other wearable devices that come with fingerprint scanners or heart rate sensors. Voice biometrics is another possibility that can be a potential mechanism for authenticating a user to a wearable device [5]. As a speaker can be readily available on wrist-worn devices, such as smartwatches, voice-based authentication may be feasible. Further, in the near future, various other bio-sensors may get incorporated into wearable devices that can be employed cleverly to design a secure and usable authentication scheme on these devices.

3.2.3 Input Inference and Side-Channel Attacks. A large variety of sensors are available in the current generation of wearable devices including audio-visual sensors (e.g., microphone and camera), motion-position sensors (e.g., accelerometer and gyroscope), and biosensors (e.g., ECG, EMG, and EEG). These sensors feature several applications including audio/video recording applications and voice/gesture-based applications. However, they can also be used by a malicious agent to

Table 3. Smartwatch Motion-Sensor-Based Input Inference Attacks Against Various Input Devices, Techniques Used, and Their Results

Compromised Input Devices	Sensor(s) Used	Techniques Used		Results
		Keystroke Detection	Keystroke Inference	
Physical keyboard (e.g., standard QWERTY keyboard)	Accelerometer, gyroscope z-axis analysis	Z-axis analysis of accelerometer	Word inference by using Point Cloud Fitting with Bayesian Model	Can shortlist a median of 24 words containing typed word-for-word length >6, the shortlist drops to a median of 10 words
	Microphone, linear acceleration	Signal processing on audio signal	Motion profiling with English words	Significant accuracy improvement in finding the text as compared to prior dictionary attacks
Physical number pad (e.g., POS)	Linear acceleration		Movement modeling with k-Nearest Neighbor (k-NN)	Probability of finding banking PINs in top 3 candidate is 65%
Soft number pad (e.g., smartphone)	Linear acceleration	Based on ground truth derived from actual key-pressed events	Set of three classifiers: Simple Linear Regression(SLR), Random Forest (RF), and k-Nearest Neighbor (k-NN)	Key inference accuracy is >90% with SLR and k-NN, while it is >80% with RF

steal the sensitive input information provided by the user through various input devices and to launch other side-channel attacks. General input devices include standard QWERTY keyboards on a normal desktop PC or any touch-enabled devices and physical number pads (e.g., POS terminal, ATM) or soft number pads on any touch-enabled devices. Several researchers have already shown that these sensors embedded within smartphones can be abused by a malicious player to steal sensitive input information [13, 110, 156] and sensitive spoken information [131]. Moreover, researchers have recently shown that the interference on the WiFi signals due to users' hand/finger movements while providing input can also be utilized to infer the sensitive input information [6, 94].

As wearable devices almost remain constantly attached to the body of the wearer, it makes them even more vulnerable to such attacks. Such input inference attacks and other side-channel attacks are described here:

- *Motion-Based Input Inference:* Very recently, several researchers demonstrated that input inference attacks could be launched with a reasonably high inference accuracy on various input devices, such as physical number pads on POS terminals [97], soft number pads on touchscreens [99], and even a desktop QWERTY keyboard [97, 149]. All these research works have leveraged motion sensors embedded on a smartwatch, one of the widely deployed wearable devices. Table 3 summarizes the different motion-based input inference

attacks on various input devices against smartwatches, the techniques used for the attacks, and their results.

The general approach of input inference attack consists of two steps: *keystroke detection* and *keystroke inference*. *Keystroke detection* estimates the start and the end of the keystroke event, while *keystroke inference* predicts the keys being pressed. Each of these steps extracts and learns the patterns of keystrokes from the motion sensors reading. Utilizing learned keystroke patterns, they detect and infer the keystrokes [97, 149]. *Keystroke detection* can also be performed by utilizing the audio signal [97] recorded by the microphone available on the smartwatch. Instead of inferring individual keys separately, some schemes infer the entire sequence of keys based on motion signals [97]. Input inference in numeric keypad can be performed using one of the state-of-the-art machine-learning algorithms, for example, k-Nearest Neighbor (k-NN), Simple Linear Regression (SLR), or Random Forest (RF) [97, 99]. However, the input inference attack on a standard QWERTY keyboard is a bit tricky and complex as motion signals captured by the smartwatch (worn only on one hand) can only reveal the information of the keystrokes residing on one half of the keyboard regions (either left or right). Though motion signals reveal only partial information about the input typed by the user, motion profiling of dictionary words [97] or Point Cloud Fitting combined with Bayesian Model [149] can be utilized to infer the word/text entered by the victim.

- *Video-Based Input Inference:* Video sensors available on the wearable devices, such as Google Glass, narrative clips, and autographer, can also be employed to infer the users' input on various input devices. Such built-in video sensors on wearables enable surreptitious video recordings while the user is providing some sensitive information to another device. With careful human analysis of such recorded video, there is a high probability that it can disclose the text typed by the user. This process of analyzing the video for disclosing the input provided by the user can also be automated by combining the various computer vision techniques, which can further enhance the capability of the attacker [15]. Moreover, computer vision techniques enable an attacker to infer the sensitive input provided by the user from a video containing the user tapping on the touch-enabled devices [139, 161].
- *Audio-Based Input Inference:* Similar to video-based input inference attacks, surreptitiously recorded audio from the wearable devices can also be analyzed utilizing the various signal processing techniques to infer the text typed by the user on a nearby terminal. Several research works [12, 64, 164] have employed traditional PC microphones to surreptitiously record the audio while the user types on a keyboard nearby, and later used the recorded audio to infer the typed text. In presented scenarios, the PC microphone remains at a distance from the keyboard. However, wrist-worn wearable devices, in particular a smartwatch, remain in very close proximity to the input devices while performing the input operation, and therefore the use of a microphone from such devices can be even more devastating than using a traditional PC microphone for such attacks. Here, an additional attacker task is to fool the user into installing a malicious application that surreptitiously records audio and pushes the recorded audio to the attacker. The same malicious application can also be used to steal the user's and bystander's spoken information, violating the wearer's as well as bystander's privacy properties underlying the wearable device.
- *Bio-Sensor-Based Inference:* Sensor that can capture brainwave signals, particularly EEG sensors, are gaining popularity in the field of gaming and entertainment. This sensor features a wide range of applications, including video games and hands-free keyboards. However, the EEG signal captured by this sensor can be abused by a malicious agent to turn it against the privacy of its user as demonstrated in [102]. A user can be easily fooled to play a cleverly designed classification game made with different images (i.e., stimuli) while wearing

an EEG-based device. A malicious entity can analyze the captured EEG signal to determine which of the presented images are associated with the user and hence can infer various private and secret information about a user, such as bank account information, PIN numbers, living area, and a person known to the user [102].

Potential Defenses.

- *Permission Restriction to On-Board Sensors:* Current mobile OSs, in particular the Android OS, do not require any permissions to access on-board motion sensors (e.g., accelerometer, gyroscope, gravity sensor). Therefore, any application can capture such sensor signals without any restrictions. These on-board motion sensors should be considered sensitive to users' privacy, and hence, a permission model should be designed that entails the security permission in order to access such sensors [106, 110]. Additionally, dynamic permission management based on the context can also be employed, such as limiting the access to the sensors when sensitive input operations (e.g., typing a PIN or password) are being performed by the user [97].
- *Privacy -Enhancing Keyboard:* The input inference attack on a touch-enabled device can be mitigated by randomizing the keyboard layout, that is, changing the position of the keys on the keyboard in every sensitive input session [141]. Randomizing the keyboard layout conceals the layout information, and hence makes it difficult for the attacker to determine the actual key being pressed even if the attacker learns the correct key-pressed position. However, this approach seems to compromise the usability of the system significantly [126] and may not be a practical defense that users would like to use. Further, this approach is only applicable to touch-enabled devices where randomizing the keyboard layout is possible, but not to physical keyboards and physical number pads.
- *Mitigating Acoustic Emanations:* The simplest approach to defeating input inference based on acoustic emanations can be to minimize the sound generated by the input devices (e.g., physical keyboards) while providing sensitive information by making the input devices as silent as possible [12]. Another approach could be to use homophonic keyboards, where each key produces the same sound upon being pressed [12]. However, this approach would require a specialized keyboard hardware. Obfuscating the audio signal generated while typing by deliberately injecting audio noises (e.g., white noise, sounds of fake keystrokes, or a combination of various noises) can be another approach to defeat such acoustic-emanation-based input inference attacks [7, 8, 164]. This approach may have an impact on the usability of the system as it can distract the user of the device or other people in the surroundings.
- *Mitigating Visual Leakage of Input/Output Devices:* Computer vision techniques can be employed to detect and discard the images containing input/output devices that can potentially reveal the sensitive information from a video recorded by the recording devices [87]. This approach can mitigate the sensitive information leakage due to surreptitious recording of image/video by video recording wearable devices, such as the Google Glass.
- *Access Control to Bio-Sensors:* To defend against bio-sensor-based, in particular EEG-based, side-channel attacks, one approach may be to prevent the exposition of raw EEG data from EEG devices to third-party applications [102]. This approach requires EEG vendors to create a restricted API that would allow a third-party application to access only certain features of the EEG signal (e.g., allowing only movement-related signals). This approach demands the wearables to have high computation power and also limits the development of a third-party application for such devices.

3.2.4 Hidden Plagiarisms. Due to their small form factor and inconspicuous nature, wearable devices have created several possibilities for students to use this emerging technology for the purpose of cheating or plagiarizing during the exams. One possibility is the use of a smartglass, or a wearable tiny video camera attached to the glass, to transmit questions wirelessly to a person outside the test room, who then relays the correct answers via a small earpiece.[36] Another possibility is the use of a smartwatch with texting capabilities to send/receive messages (could be questions/answers) surreptitiously during the exam.[37] Some smartwatches also feature the ability to read text or PDF files. Such ability can be employed by the students to store and use the cheat-sheet during the exams.[38] The wearable devices would be even more inconspicuous in a remote exam proctoring session (e.g., ProctorU and KRYPTERION Online Proctoring) where the proctors are not physically present for watching over the test takers during the test. In such scenarios, the proctor monitors the test remotely over the Internet (usually using a webcam). As wearables are becoming inconspicuous, the remote presence of proctors would make it even harder for them to detect test takers cheating through wearables.

The test takers can also work collaboratively utilizing wearable devices using the cloud-based features. For example, the recent work of [105] has designed *ConTest*, a cloud-based smartwatch application, that enables dishonest students to cooperate on multiple-choice exams in real time stealthily. *ConTest* consists of three components: *smartwatch app*, *smartphone app*, and *cloud server*. Smartwatch app enables an individual to submit his or her response and view the collaboratively decided answer. Smartphone app relays the data between a smartwatch and a central cloud service. Cloud server, a cloud-based central service, collects and aggregates the responses provided by individual students. For each question, the cloud application determines the most common response and circulates it to each individual as necessary through smartwatch. To make it difficult for the proctor to notice the ongoing plagiarism activity, the correct date and time are displayed on the watch's screen. It also shows the inverted small groups of noncritical pixels on the watch's face that indicate the question and the corresponding answer. Beyond exam settings, such an application may also be adapted to gain underhanded benefits in other scenarios like gambling.

Potential Defenses. Banning high-tech wearables from exam rooms could be a potential solution to prevent dishonest students from cheating using wearable devices. Since wearables like smartwatches are becoming common and difficult to spot, it may not be questionable to ban such high-tech devices. Instead, replacements, such as wall clocks for watches, can be provided in the examination centers. The Graduate Record Examination (GRE) has adopted a policy that prohibits the use of all types of watches, including digital and smartwatches, in its testing room.[39] However, the policy to ban such high-tech devices could be annoying for wearers as they may not wish to give their belongings away to others during the exams, raising a privacy concern.

Another simple solution could be implementing a *software-based restriction* that restricts the usage of wearable devices in a specialized environment [105]. For example, an *"Exam Mode"* on the devices can be activated by the external signal from the examiner, or when the device senses being in a special environment, that restrains the wearer from using restricted features available on the device. However, such an approach has only been discussed in the research literature and has not been designed and evaluated. Future work is needed to determine whether it is feasible to design a wearable device with flexible, safe, and guarantee-able restriction policies.

[36] High-tech cheaters pose test – http://goo.gl/9QoRMt.
[37] Thai exam cheating triggers phone-watch ban – http://goo.gl/A2nFup.
[38] Student disciplined for cheating on exam with smartwatch – http://goo.gl/czU9NC.
[39] Graduate Record Examination (GRE) – http://goo.gl/EDe6kq.

Since wearable devices are gaining popularity and are evolving with decreasing size and detectability and increasing computational power and connectivity, the aforementioned high-tech cheating may become more widespread in the near future. Therefore, research work is highly needed to design policies or software-based mechanisms to restrict the use of wearable devices to prevent the wearer from gaining such underhanded benefits through the use of wearables.

3.2.5 Accidental Leakage to Online Services. With a multitude of built-in sensors, wearable devices continuously collect information about the user and his or her surroundings and often outsource the collected information to cloud storage and third-party services, or some even automatically synchronize with online social media. Many of the wearable devices (e.g., health monitoring devices) require them to be online in order to operate fully. In other words, the user can utilize the device properly only after agreeing to the service privacy policies [116]. Sometimes, users forget that they have granted the data access permission to the applications on the wearables, which continuously synchronize the data to third-party/cloud services. The information collected by the wearables may contain some information that is private to the users that they may not wish to share with anyone. The properties of wearables to automatically synchronize with online/cloud services and social media may threaten the privacy of the user. For instance, the sexual activity of some of the Fitbit's users had been exposed to online services due to Fitbit's default settings in the past.[40]

Potential Defenses. Creating an ideal platform where wearables are fully capable of operating offline would be one possible defensive approach to prevent accidental leakage of the sensitive information to online services and social media. This approach could be achieved by utilizing the increasing computational and storage capacities of mobile devices. That is, a wearable platform can be built that stores and analyzes the data locally on a user's smartphone, which alleviates the concerns regarding third parties holding and processing the data. In situations where cloud-based services are needed, clear and precise information about the data processing, retention, and sharing policies should be given to the user and the user's consent should be sought. Also, to minimize the risk of user privacy violations, as little personal identification information as possible should be requested and stored [116].

It should also be ensured that all the data collected and stored by the service provider is not exposed to others. One approach to ensure this is to preprocess and encrypt all the data on the user's end before transmitting it to the provider. Another approach could be to transmit only necessary data or features required to provide proper functionality to wearables. Such approaches are commonly referred to as privacy-preserving approaches. In such a scenario, providers have to perform all the necessary computation over the encrypted data, commonly known as privacy-preserving querying and computation. Several works have been done in this direction, including those on machine-learning algorithms for computation over encrypted data [3, 20, 46, 146, 153, 160], encrypted query processing [18, 75, 117, 118, 135, 140], privacy-preserving image search and retrieval [1, 32, 51, 73, 98, 155], and so forth. However, as these techniques require cryptographic operations that may be computationally expensive, only a few of these schemes (e.g., [1, 135]) are tailored for resource-constrained devices like wearables. Further research is needed in this context to explore and design optimized privacy-preserving querying and computation schemes that are applicable for such devices.

For a statistical dataset, instead of encrypting the whole dataset and applying queries over encrypted data, *differential privacy* [47] can be applied to ensure the privacy of an arbitrary individual involved in the dataset. Differential privacy provides aggregate statistical information about

[40]The activity tracked by Fitbit shows up in Google search results – http://goo.gl/84lWDa.

the dataset without compromising the privacy of the individuals. Such privacy on the statistical dataset can be achieved through (1) query restriction (e.g., restricting size of query results, suppression of values to smaller size [38, 42]) and/or (2) data perturbation (e.g., adding noise to the values of the dataset or to the result of a query, attribute swapping, data resampling by imputation [3, 50]). We believe that *differential privacy* techniques are appropriate to preserve the privacy of the individuals in a statistical dataset in the context of wearables.

A runtime permission model can be employed to address the issue of users forgetting that they granted permission to the application.[41,42] The runtime permission model asks the user for required permissions as they become necessary during application use, not when a user installs the application. However, asking the user for required permission every time an application accesses resources may be annoying to the user. A more usable and less annoying permission model may be the one that displays a notification about agreed-upon permissions on the wearables whenever the application tries to utilize them. Displaying the notification may serve as a reminder about the permissions granted to a specific application.

3.2.6 Hijacking Communication Links. Most of the wearables are usually linked wirelessly with either a companion mobile device (smartphone) or a personal computer to offer full functionality. This wireless communication link is also one of the attack vectors that an adversary can utilize to harm the users. Carelessly designed communication protocols may allow an adversary to perform various malicious activities including eavesdropping over all the communication between wearables and the connected devices, data tampering, malicious data injection, and denial-of-service attacks. For example, a poorly designed Fitbit communication link during its early stage allowed an adversary to discover any Fitbit tracker device in range and the associated fitness information stored on the device as demonstrated in [120]. An attacker who has learned certain information about the format of the memory bank and opcode instructions can even modify any real-time fitness data stored in neighboring trackers [120]. This attack can further be extended to launch a form of denial-of-service attack by modifying the real-time statistics of the user, which prevent the user from accessing the original statistics. Moreover, by continuously querying the trackers, batteries can be made to drain out at a faster rate.

The authors of [120] also designed *"FitLock,"* a scheme to prevent the vulnerabilities mentioned earlier associated with Fitbit. However, the research presented in [163] discovered that the protocols composing *FitLock* still suffer from vulnerabilities. Specifically, it fails to encrypt the identity of a Fitbit tracker through which an adversary can track the device, and thereby a person wearing it. The attacker can send the tracker's identity to the web server repeatedly and retrieve a set of responses. By relaying these responses to the tracker, the attacker can impersonate the web server. Fitlock protocols also lack mutual authentication between the web server and the tracker device, due to which anyone in possession of the tracker device can register it to the web account by just sending its identifier.

Potential Defenses. During the entire session of the communication, sensitive and identifying information should not be sent in clear-text—some form of encryption mechanism should be employed. To defend against impersonation attacks, mutual authentication mechanisms should be implemented. Overall, secure communication protocols should be implemented to prevent an attacker from eavesdropping and hijacking the communication link. Several secure device pairing protocols exist, such as the manual authentication protocol [58], the ephemeral pairing protocol [70, 107], the *"Diffie-Hellman with Visual Comparison of Short Strings"* protocol [25], and the

[41] Run Time Permissions, Android – https://goo.gl/9FTnEL.
[42] Requesting Permission, iOS – https://goo.gl/W4A59o.

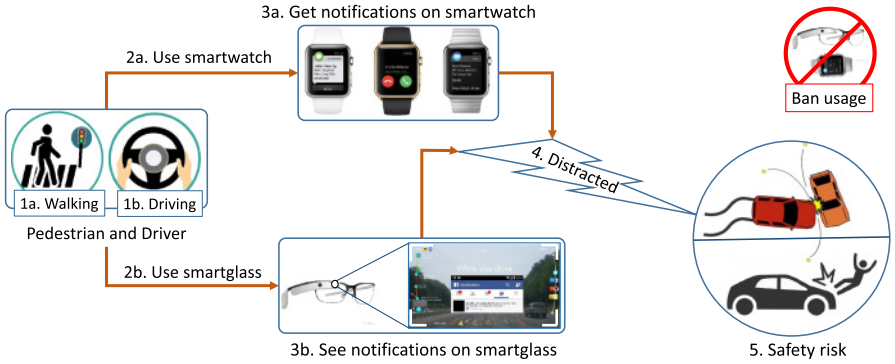

Fig. 4. Safety risk instances of wearable usage. A pedestrian while crossing the street or a driver while driving gets distracted from the notifications on the smartwatch/smartglass, leading to safety risks.

"SAS-Based Authenticated Key Agreement" protocol [148], that can and should be used for establishing a secure communication channel between the wearable and the companion device. The use of these protocols can prevent the aforementioned vulnerabilities. However, many of these protocols require user involvement to establish secure sessions, and thus the security and usability implications of such user involvement should be investigated further in the context of wearable devices.

3.2.7 Device Integrity. Earlier in this section, we presented several threats against or of using wearable devices and discussed corresponding potential mitigation strategies against them. These mitigation strategies hold true only when the integrity of the device is assured. Without device integrity, none of these strategies would be reliable in the real world. For instance, defenses presented to mitigate the privacy threat of wearable cameras work only if the device has not been compromised (i.e., the internal firmware of the device has not been modified or replaced). So, device integrity assurance (checking and verification) is a fundamental requirement of the wearable devices before the implementation of any security schemes on the devices. Device integrity is attained through remote attestation, a technique that ascertains the current state of the computing device. Various remote attestation techniques have been proposed in the literature: some are hardware based [88, 114, 133], some are software based [9, 81, 96, 134], and some are hybrid techniques [21, 48, 52, 84, 86] that combine hardware and software. They differ from each other greatly in terms of security, adversarial models, communication, and device feature assumptions.

Hardware-based techniques can be secure and effective, and applicable to the devices that can accommodate additional monetary cost and power consumption. Due to the resource-constrained nature of wearables, such hardware techniques may not work well on such devices. Software-based techniques, on the other hand, require no additional hardware and involve minimal overall costs that seem to be appealing for wearable devices. However, they offer only limited (often uncertain) security guarantees and are sometimes restricted to some specific settings. Hybrid techniques lie in between these two approaches that involve hardware-software codesign and offer better security than software-based approaches. Some of the software-based and hybrid approaches may be reasonable to ensure device integrity on wearables. However, wearables bring forth several challenges toward remote attestation because of their resource-constrained and heterogeneous nature and small form factors. First, the attestation schemes should be lightweight and applicable for resource-constrained devices. Second, the scheme should be scalable to multiple numbers of wearable devices. Third, the scheme should support heterogeneous devices including

head-worn, eye-worn, and wrist-worn devices. Being resource-constrained devices, implementation of such attestation schemes may not be well secured and can be exploited, for example, through verifier impersonation or denial-of-service attacks against honest provers. So one challenge is to design a well-secured remote attestation scheme. Rigorous research work is needed to design a lightweight and secure device integrity checking and verification mechanism for wearable devices.

3.2.8 Safety Risks. Beyond raising security and privacy vulnerabilities, the wearable devices also introduce the risks to wearers' safety. In some instances, a wearable device can introduce a higher degree of risk than a nonwearable device. As wearable devices remain attached to the body of the wearer, they place the potential source of harm (e.g., a distracting notification) near the wearer. For example, the use of a smartwatch or a wearable glass while driving has the potential to distract the wearer and can create a safety concern.

Several studies [23, 24, 45] have already shown that the use of mobile phones while driving has negative consequences on driving behavior and hence the use of mobile phones has been prohibited while driving in most places. Recently, a series of work [59, 60] performed a driving simulator study to investigate the comparative degree of distraction with smartwatches and smartphones in terms of engagement time with the devices, drivers' glance patterns, and brake response time when there is a notification on the device. The key findings from these studies are listed as follows:

- The wearer gets engaged faster with the smartwatch as compared with the smartphone but takes a longer time to read the smartwatch notification.
- The duration of individual glances as well as the number of glances while driving using the smartwatch is greater than that while using a smartphone.
- The percentage of time the eyes are off-road is higher when receiving notification on the smartwatch compared to receiving notification on the smartphone.
- The brake response times before a braking event from a lead vehicle are longer when receiving notifications on the smartwatch compared to receiving no notifications and compared to receiving notifications on the smartphone.

These findings indicate that the use of a smartwatch increases the degree of drivers' distraction when compared to the use of a smartphone. This result is attributed to the limited-size display screen on the smartwatch. The limited screen on a smartwatch requires multiple views across multiple windows, and hence more manual interactions to go through each window. While driving, the user is already occupied with the driving task both physically and visually, and this additional burden due to the limited screen display may create safety risks. The same situation may arise while crossing a street where the pedestrian may get distracted with a smartwatch notification to a higher degree.

A smartglass, like the Google Glass, features a hands-free interface (i.e., voice based) for text messaging and near-eye display for viewing the messages. Due to these features, the wearable glass might seem to offer a distraction-free driving scenario. However, several simulated driving studies [66, 67, 129] have demonstrated that though they serve to moderate, they do not eliminate the distraction in terms of speed, lane changing, and brake response time. Wearable glasses with speech-based interfaces impair less compared to hand-held texting, as they allow a hands-free interaction. However, they still significantly affect driving performance in terms of larger deviations in speed, lane positioning, and brake response time [66, 129]. Further, the use of near-eye display can hinder visual abilities, which may distract the drivers since the driver needs to pay attention simultaneously to the display and to the road. Such displays can also impair the visual processing of

a driver by overlapping the visual information while driving. The study of [67] demonstrated such a visual impairment due to the use of near-eye display while driving in terms of larger variation in lane keeping.

Potential Defenses. As wearable devices such as smartwatches, wristbands, and augmented reality glasses have gained popularity recently, legal policies and rules on the use of such devices while driving are not yet clear. For instance, many state laws in the United States prohibit the use of "hand-held devices" while driving. However, such laws do not cover wrist-worn smart devices (e.g., smartwatches) explicitly because they are neither hand-held nor hands-free. Similarly, wearable glasses are not hand-held, but they are found to create significant distractions to drivers through their use. In this light, clear guidelines and policies should be designed and implemented regarding the use of wearable technologies in the driving context. There are wearables other than smartwatches and wearable glasses, and many new wearables with new features and functionalities are forthcoming. Legal guidelines on the use of such devices should be crafted by law enforcement before these devices become widespread and endanger traffic safety. Beyond driving safety, another concern is pedestrian safety while using wearable devices. No studies to our knowledge, however, have been reported in the context of pedestrian distractions with the use of wearable devices. Further work is needed in this direction.

Besides the legal dimension, software-based mechanisms may also be designed such that they can avoid the distraction while performing a critical task on the road or otherwise. For example, an application could be designed that can automatically sense if the user is performing a critical task (e.g., crossing the street or driving) and then delay the distracting notifications on the device until the critical task has been completed. Further work is warranted to design and evaluate such "distraction prevention" apps for wearable devices.

4 SECURITY, PRIVACY, AND SAFETY ENHANCEMENTS IN EXISTING SYSTEMS

While wearables open up the potential for abuse and offensive usage, they may also facilitate the enhancement of existing security, privacy, and safety paradigms in unique ways while increasing, or at least preserving, the system's usability. One such enhancement pertains to the problem of user authentication. Wearable devices could be used to build *brainwave authentication* (authentication based on human thoughts) and *zero-effort (de)authentication* (promptly and transparently recognizing when to deauthenticate a previously authenticated user). They can also be used to improve the usability and/or security of traditional password authentication and that of *two-factor authentication*. These enhancements have become possible due to the increasing availability of physiological and motion-position sensors in wearable computing. Another defensive application of wearable computing relates to the wearer safety schemes, including *pedestrian risk identification* and *driver drowsiness detection*. In this section, we discuss such enhancements brought forth by the emergence of wearable computing to the context of authentication and user safety paradigms.

4.1 Authentication

User authentication is a process to determine whether a user is indeed who he or she claims to be. Various types of discriminating characteristics are used to authenticate the user. Based on the use of these characteristics, authentication approaches can be categorized into three classes [104]: (1) *"Knowledge-Based Authentication,"* which relies on something that the user *knows* (e.g., password, PIN, pattern); (2) *"Possession-Based Authentication,"* which relies on something that the user *has* (e.g., hardware tokens such as phone, wristband, smartcard token, or software tokens such as an application installed on a cell phone); and (3) *"Biometric-Based Authentication,"* which

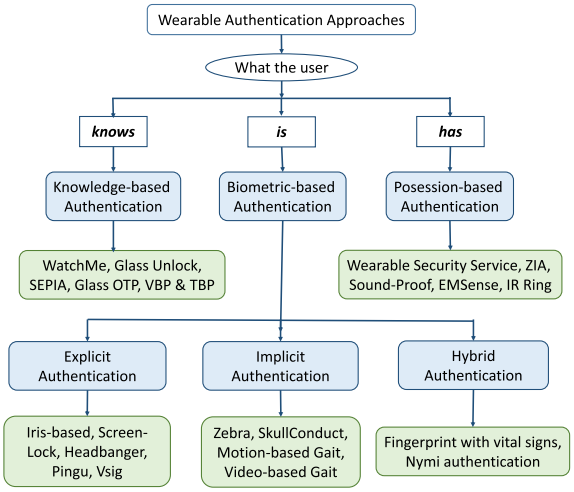

Fig. 5. Classification tree of wearable authentication approaches. The leaf nodes (green colored) show the examples of each approach.

is based on something that the user *is* or *does* (e.g., fingerprint, retina, voice, face, voice, keystroke dynamics, gait patterns, hand gestures). Our study of wearable authentication is also structured according to this established classification scheme as presented in Figure 5.

Table 4 systematizes the wearable authentication schemes considered in this literature survey with respect to usability, deployability, and security criteria as described in "The Quest to Replace Password" [19]. "*Server Compatible*" and "*Browser Compatible*" properties under deployability criteria are not applicable in our comparison since wearable authentication schemes considered are not web-based authentication schemes; rather, they are either completely client-side authentication schemes (i.e., authentication for wearables) or the schemes that employ wearables as a token to authenticate the user to external systems or services. One exception is "Sound-Proof," which is a web-based authentication system. Sound-Proof authors envisioned the usage of a smartwatch instead of a smartphone for authentication purposes. Sound-Proof is both *Server Compatible* and *Browser Compatible* as it does not require any changes to the browser or the server side. It only requires the ability to communicate with the server and the implementation of a correlation engine on the smartwatch.

4.1.1 Wearable Knowledge-Based Authentication. Textual passwords are a widely used knowledge-based authentication approach. They are widely accepted because of their intangible nature; that is, they can be easily and simply issued, changed, shared, and revoked [17]. However, researchers [83, 123, 152, 157] have demonstrated that the passwords have several well-known limitations: passwords, especially random ones, are often difficult to memorize; memorable passwords typically have low entropy in practice, which makes them susceptible to dictionary attacks; and passwords are vulnerable to "shoulder surfing" and observation attacks. Wearable devices have the potential to address these limitations by providing the input strategies that improve usability and the remembrance or recall of passwords and are also resistant to shoulder surfing.

For example, wearable devices can be used as a second factor in the traditional two-factor authentication scheme (in which a verification code is sent to a smartphone) that may offer improved usability during the authentication process. When using a smartwatch, as opposed to a smartphone, as the second factor, it would be much easier for the user to view and copy the code to

Table 4. Comparing Wearable Authentication Schemes with Usability, Deployability, and Security Criteria as Used in "The Quest to Replace Passwords" [19]

Category	Scheme	Reference	Type	Usability								Deployability				Security											
				Memorywise- Effortless	*Scalable-for-Users*	*Nothing-to-Carry*	*Physically-effortless*	*Easy-to-Learn*	*Efficient-to-Use*	*Infrequent-Errors*	*Easy-Recovery-from-Loss*	*Accessible*	*Negligible-Cost-per-User*	*Mature*	*Non-proprietary*	*Resilient-to-Physical-Observation*	*Resilient-to-Targeted-Impersonation*	*Resilient-to-Throttled-Guessing*	*Resilient-to-Unthrottled-Guessing*	*Resilient-to-Internal-Observation*	*Resilient-to-Leaks-from-Other-Verifiers*	*Resilient-to-Phishing*	*Resilient-to-Theft*	*No-trusted-Third-Party*	*Requiring-Explicit-Consent*	*Unlinkable*
Knowledge-based	*WatchMe*	Van Vlaenderen et al. (2015)	2	¬	¬	¬	¬	▪	▪	¬	▪	▪	¬	¬	▪	▫	▫	¬	¬	¬	¬	¬	▪	▪	▪	▪
	VBP & TBP	Yadav et al. (2015) and Bailey et al. (2015)	1	¬	¬	▪	▫	▪	¬	¬	▪	¬	▪	¬	▪	▪	▫	¬	¬	¬	¬	¬	▪	▪	▪	▪
	Glass Unlock	Winkler et al. (2015)	2	¬	¬	¬	¬	▫	¬	¬	▪	¬	▫	¬	▪	▪	▫	¬	¬	¬	¬	¬	▪	▪	▪	▪
	SEPIA	Khan et al. (2015)	2	¬	¬	¬	¬	▫	¬	¬	▪	¬	¬	¬	▪	▪	▫	¬	¬	▪	¬	¬	▪	▪	▪	▪
	Glass OTP	Chan et al. (2015)	1	▪	▪	▫	¬	▪	▪	▪	▪	¬	▪	¬	▪	▪	▪	▪	▪	▪	▪	▪	▪	▪	▪	▪
	Brainwave-based	Ashby et al.(2011) and Chuang et al. (2013)	2	¬	¬	¬	▪	▪	▪	¬	▪	▪	¬	¬	▪	▪	▪	▪	¬	¬	¬	▪	▪	▪	▪	¬
Biometric-based	*Iris-recognition*	Lee et al. (2004) and Wang et al	1	▪	▪	▪	▫	▪	▫	¬	¬	▫	▪	¬	▪	▪	¬	▪	¬	¬	¬	¬	¬	▪	▪	¬
	Screen-Lock	Google Inc. (2016)	1	¬	¬	▪	¬	▪	▪	▫	▪	▪	▪	¬	¬	¬	¬	▪	¬	¬	¬	▪	▪	▪	▪	▪
	Headbanger	Li et al. (2016)	1	▪	▪	▪	▪	▪	▫	¬	▫	¬	▪	¬	▪	¬	¬	▪	¬	▪	¬	▪	▪	▪	▪	▪
	MotionAuth	Yang et al. (2015)	1	¬	¬	▪	▪	▪	▫	¬	▫	▪	▪	¬	▪	¬	¬	¬	¬	▪	▪	▪	▪	▪	▪	▪
	Pingu	Sajid and Cheung (2015)	2	▪	▪	¬	▪	▪	▫	▫	▪	▪	¬	¬	▪	▫	¬	▪	▪	¬	▪	▪	▪	▪	▪	¬
	Vsig	Roshandel et al. (2014)	1	▪	▪	▪	▪	▪	▫	▫	▪	▪	▪	¬	▪	▫	¬	▪	▪	¬	¬	▪	▪	▪	▪	¬
	Motion-based-Gait	Gafurov et al. (2008, 2007a, 2011) and Li et al. (2016)	1	▪	▪	▪	▪	▪	▪	¬	▫	¬	▪	¬	▪	¬	¬	▪	▪	¬	¬	▪	▪	¬	¬	¬
	Video-based-Gait	Shiraga et al. (2002) and Shen et al. (2015)	1	▪	▪	▪	▪	▪	▪	¬	▫	¬	▪	¬	▪	¬	¬	▪	▪	¬	¬	▪	▪	¬	¬	¬
	Touch-based	Chauhan et al. (2016)	1	▪	▪	▪	▪	▪	▪	▫	▫	▪	▪	¬	▪	¬	¬	▪	▪	¬	▪	▫	▪	▫	¬	¬
	Zebra	Mare et al. (2014)	2	▪	▪	¬	▪	▪	▪	▫	▪	▪	¬	¬	▪	¬	¬	▪	▪	▪	▪	¬	▪	¬	¬	▪
	Electric profile	Holz et al. (2015), Sato et al. (2012), and Cornelius et al. (2014)	2	▪	▪	¬	▪	▪	▪	▫	¬	▪	¬	¬	▪	▪	▪	▪	¬	¬	¬	▪	▪	¬	¬	
	SkullConduct	Schneegass et al. (2016)	1	▪	▪	▪	▪	▪	▪	¬	¬	▪	▪	¬	▪	▪	▪	▪	¬	¬	¬	▪	▪	▫	¬	
	Hybrid Authentication	Ojala et al. (2008) and Nymi (2014)	2	▪	▪	¬	▫	▪	▪	¬	¬	▪	¬	▪	▪	▪	¬	▪	¬	¬	¬	¬	▪	▪	¬	
Possession-based	*Wearable Security Service*	Al-Muhtadi et al. (2001)	2	▪	▪	¬	▫	▪	▪	▪	▪	▪	¬	▪	▪	▪	▪	▪	¬	¬	¬	¬	▪	¬	¬	
	Sound-Proof	Karapanos et al. (2015)	2	▪	▪	¬	¬	▪	▪	¬	▪	▪	¬	¬	¬	▪	¬	¬	¬	▪	¬	¬	▪	¬	¬	▪
	ZIA	Corner et al. (2002), Nicholson et al. (2006), Sun et al. (2008), and Cha et al. (2015)	2	▪	▪	¬	▪	▪	▪	▪	▪	▪	¬	¬	¬	▪	¬	▪	▪	▪	¬	▪	¬	▪		
	Wearable Key	Matsushita et al. (2000)	2	▪	▪	¬	▪	▪	▪	▫	▪	▪	¬	¬	▪	▪	▪	¬	¬	¬	¬	¬	¬	¬	¬	¬
	IR ring	Roth et al.(2010)	2	▪	▪	¬	▪	▪	▪	▪	▪	▪	¬	¬	▪	▪	▪	▪	▪	¬	¬	¬	▪	¬	▪	¬
	EMSense	Laput et al. (2015)	2	▪	▪	▫	▪	▪	▪	¬	▪	▪	¬	¬	▪	¬	▪	▪	¬	¬	¬	¬	▪	¬	¬	

"Type" indicates if the authentication scheme (1) is for wearables or (2) uses wearables as an authentication token.
▪ = "offers the benefit"; ▫ = "almost offer the benefit"; ¬ = "does not offer benefit".

the terminal. Consequently, the use of a smartwatch or other wearables in traditional two-factor authentication may help increase the adoption of such schemes in practice. Wearable devices can also be used to design an input strategy that can conceal the input from the observer, improving the security of the scheme. "*WatchMe*" [147], for example, is an approach of providing input for smartwatches. In particular, *WatchMe* utilizes the camera on the smartwatch and advance image-processing techniques to enable a user to provide input by drawing on everyday objects (e.g.,

writing on a piece of paper using a pen, writing on a wall using a finger or laser pointer). The authors have envisioned the use of this technique for authentication—the user providing secret input using the finger or laser pointer. As finger/laser pointer movement is discrete in nature, the authors argued that the entered data will be concealed from observers.

Augmented reality glasses such as Google Glass that guarantee a fully private personal display are the best fit for designing authentication systems that are resistant to shoulder-surfing attacks. Utilizing the private display property of wearable glass, Yadav et al. Yadav et al. [157] proposed *"Touch-Based PIN (TBP)"* and *"Voice-Based PIN (VBP)"* authentication schemes, which are resistant to shoulder-surfing attacks. In their schemes, a keypad with random mapping of input digits is shown in the private display of the glass. In order to authenticate the user, the scheme requires the user to tap or utter the cipher PIN corresponding to the actual PIN in the headset. As attackers cannot observe the mapping of digits, information about the actual PIN remains concealed during the PIN entry process. Both TBP and VBP seem to surpass the built-in screen-lock scheme, as they achieved a success rate (successful log-in attempts) of more than 80% with TBP or VBP and only a 68% success rate with the built-in scheme. Bailey et al. Bailey et al. [14] presented a similar voice-based authentication scheme on smartglass. In their system, instead of a randomly mapped input grid, a randomly chosen simple mathematical operation (e.g., addition, subtraction) is displayed on the private display. The user applies this operation to his or her PIN digits and utters the result. As the attacker is unable to observe the operation that was applied, he or she cannot derive any information about the PIN even after listening to the spoken input.

Private display of the smartglass can also be utilized to design a shoulder-surfing-resistant authentication system for external devices, such as a smartphone, an ATM, or point-of-sale terminals. For example, "*Glass Unlock*" [152] is an authentication scheme that utilizes the private display of the glass to unlock the smartphone. The authentication mechanisms that have already been deployed in the smartphone, such as PIN and unlock patterns, are vulnerable to various real-world attacks: smudge attacks [13] and shoulder-surfing attacks [41]. To prevent such attacks, *Glass Unlock* leverages the private display of a smartglass to unlock the phone's lock screen. *Glass Unlock* hides the lock information (e.g., PIN digits) on the phone and instead shows it on the glasses' display. The input screen (say, numeric pad) on the phone shows an empty button while the randomized layout of buttons would be visible on the glasses. Randomizing the input layout and hiding the input screen layout makes *Glass Unlock* resistant to observation attacks, such as shoulder surfing, camera-based eavesdropping attacks, and smudge attacks. Similar to *Glass Unlock*, *SEPIA* [82] also uses a smartglass for PIN-based authentication at an ATM or at a point-of-sale terminal in a way that is secure against shoulder-surfing and observation attacks. *SEPIA* is claimed to be a *"secure obfuscated PIN authentication protocol."* SEPIA requires a user to prove its colocation with the terminal to the cloud service by scanning the QR code using smartglass. The cloud service then sends a PIN template to smartglass for point-of-sale authentication. Obfuscating the PIN by generating a new PIN template on the glass for every session while accessing the point of sale may make *SEPIA* secure against shoulder-surfing and camera-based eavesdropping attacks. However, it may make it harder for the users to input their PINs, which may lower the usability of PIN-based authentication.

Cameras in smartglasses can also be utilized by One-Time-Password (OTP) schemes for unlocking wearable devices. For instance, "*Glass OTP*" [29] is an OTP-based authentication scheme that utilizes a glass camera to unlock the device. In Glass OTP, a companion application installed on the user's phone generates a time-based OTP using a private key shared with the glass and embeds it in a QR code. The lock screen application on the glass then scans the QR code using its camera, verifies the OTP, and unlocks the glass.

A new emerging class of wearable knowledge-based authentication schemes leverages the thought of the user as passwords. Several research studies [100, 111, 112, 119, 145] have demonstrated the feasibility of authenticating a user based on the user's thought, in particular brainwave signals, employing clinical-grade multichannel EEG sensors. Two recent studies by Ashby et al. [10] and Chuang et al. [33] have demonstrated the feasibility of authentication based on brainwave signals with a high accuracy level (greater than 97%) using a consumer-grade single-/multichannel EEG headset (e.g., Neurosky or Emotive headsets). The authentication techniques require the user to perform a single step of executing a mental task while wearing a brainwave-sensing headset. The mental task includes choosing a secret, for example, imagining certain motor movements, mentally singing a previously selected song, or counting the objects of a particular color. Such thought as a password-based authentication system may be vulnerable to impersonation attacks. However, the study in [78] shows that brainwave authentication is robust against impersonation attacks (impostor acceptance rate is fairly low at 4.5%). There are other benefits to the brain authentication techniques. They could avoid the shoulder-surfing problem associated with most "something you know" schemes. Moreover, they do not seem to possess the same vulnerabilities as other biometric authentication systems. For instance, fingerprint-based authentication can be defeated by cleverly using putty and gelatin moldings or advanced imaging and printing technologies [30]. Brainwave authentication, in contrast, seems secure against such strategies since stealing a user's brain signals might be very difficult.

These examples highlight the potential of using various characteristics, such as built-in sensors (e.g., camera and EEG sensor) and private display of eyeglasses, of wearable devices to conceal the passwords from bystanders while at the same time improving the usability and the remembrance of passwords or PINs.

4.1.2 Wearable Biometric-Based Authentication. This class of authentication scheme relies on *what the user is*. Specifically, it is based on the certainty that some set of physiological and behavioral features of the users are unique to individuals and can be used to distinguish one person from another reliably. As a wide range of sensor modules are available in today's wearable devices that can extract various physiological and behavioral features of the user, they make wearables suitable for a variety of authentication schemes, including an *explicit* authentication scheme that requires a dedicated user action, an *implicit* authentication scheme that doesn't require any dedicated user action (they are often *continuous* in nature), and a *hybrid* authentication scheme that combines both explicit and implicit authentication features.

(1) *Explicit Authentication:* This type of authentication scheme is conceptually simple and widely popular. It requires a dedicated user action to measure the bodily characteristics. Researchers have explored a wide variety of mediums to design explicit authentication. For instance, the recent development of smart eyeglasses has stimulated research work on iris recognition systems [91]. Iris recognition systems have been deployed in many contexts other than authenticating the user to wearables such as UAE's IRIS border control system [40]. However, the underlying technology still faces many practical challenges for wearable devices, and research has been focusing on addressing these issues. For example, Lee et al. [91] presented a method to eliminate distortions from the radial lenses used in head-mounted cameras, thereby improving the accuracy and reliability. To ensure robustness against fake iris or imitation attacks as demonstrated in [125], Wang et al. [150] combined a pupil size consistency check with an iris recognition system, thereby making it more secure and robust.

Several research works have used touch and movement (finger, hand, or head movement) as a channel to design minimal-effort explicit authentication systems. For example,

"*Bulletproof*" [44] and *"screen lock"* [62] are gesture-based authentication schemes that unlock the eyeglasses based on a user's gesture pattern on the glass touchpad. Gesture pattern in *screen lock* is a combination of four touch gestures derived from a pool of 10 predefined gestures. The pool of gestures contains tap or swipe gestures, which can be created using either one or two fingers. In the case of a forgotten pattern, a user can reset the glass *lock screen* using a QR code that can be obtained by logging into the glass website. This technique is highly usable because it only requires a free hand and a sense of touch. However, it is susceptible to shoulder surfing as the finger movement during the gesture pattern input is highly visible to others. "*Headbanger*" [95] is another behavioral authentication scheme based on unique head movement patterns of the user wearing the headset in response to an external audio stimulus. "*MotionAuth*" [159] uses a set of hand gestures to authenticate the user wearing a wrist-worn smart device. Through the wrist-worn device, *MotionAuth* collects movement data during gesture performance and uses it to verify the user identity with a high level of accuracy (2.6% error rate). *"Pingu"* [127] and *"VSig"* [122] are in-air hand-gesture-based authentication schemes that require a user to make a virtual 3D signature in the air. *Pingu* collects temporal patterns during the making of a 3D signature through the ring equipped with a set of sensors and identifies/recognizes the user with a high level of accuracy (100% with 24 users). On the other hand, *VSig* records the video during in-air 3D signature creation, tracks the fingertip to reconstruct the signature, compares it with prestored signatures of the individual, and grants access to the user.

(2) *Implicit Authentication:* Motion sensors have frequently been used as a channel to design implicit authentication schemes. Movements of a different part of the body while doing regular activities can be monitored by attaching motion sensors to various parts of the body. The viability of extracting different movement signals and using them for authentication purposes has been investigated in various research works: arm-mounted sensors to capture the arm swing [57], ankle-mounted sensors to capture foot movement [53], and sensors mounted at the lower leg [54], hip [55], and head [95] to capture the gait. The studies cited have demonstrated that the movement signals can be utilized to distinguish one person from another with a reasonable level of accuracy. The user recognition accuracy based on movement signals presented in the literature cited previously relies on different test scenarios and ranges from 68% to 98%. Wearable cameras have also been used to devise an implicit authentication mechanism by extracting gait patterns from a video stream [136, 137]. Researchers reported that a video-based approach for authentication has the high recognition accuracy: a 5.6% equal error rate with a pool of 39 participants. However, as the techniques rely on observable bodily movements, gait-based authentication is vulnerable to impersonation/spoofing attacks [56].

Touch and movement have also been employed to design an implicit and unobtrusive continuous authentication scheme for smart eyeglasses. For instance, Chauhan et al. [31] presented a continuous authentication scheme based on touch gestures on the built-in touchpad on the side of Google Glass. They demonstrated that continuous authentication on glasses based on touch gesture is both computationally and accuracy-wise feasible. Wearable devices have also been employed to achieve continuous authentication (or *de-authentication*) for external devices. "*ZEBRA*" [101], for instance, continuously yet transparently reauthenticates the user to the terminal. *ZEBRA* requires a user to wear a bracelet equipped with sensors on his or her mouse-holding hand as a token for continuous authentication. The bracelet is wirelessly connected to the terminal that compares

the sequence of events it observes (e.g., typing, scrolling, and hand movement between mouse and keyboard) with the sequence of events inferred using the bracelet sensor's measurements. When these two sequences do not match, the terminal de-authenticates the logged-in user. Though these continuous authentication schemes appear to be compelling because of their transparent and unobtrusive nature, as the underlying techniques rely on observable hand movements, they are also vulnerable to impersonation attacks. For example, recent work in [74] has devised an effective attack strategy—a human attacker observes a victim at the nearby terminal and opportunistically mimics only a subset of the victim's activities (e.g., keyboard events) at the authenticating terminal—that can defeat the *ZEBRA* scheme. With this strategy, the authors have demonstrated that the opportunistic attacker has a high probability of breaking the scheme. These studies show that though zero-effort continuous authentication is a compelling notion, it is susceptible to observation attacks and correctly designing such schemes is highly challenging.

Addressing the threat of impersonation attacks against the observable bodily-movement-based authentication scheme, researchers have also considered the use of unobservable bodily characteristics, such as electric profile and the frequency response of a user's skull in response to an audio signal, in designing implicit authentication schemes. For example, *"Bioamp"* [71] is a watch prototype that leverages the electric profile of a user through the wrist-worn device to authenticate the user. *Bioamp* extracts the impedance from the user's wrist, encodes it as an electrical signal, and transmits it to touch-enabled devices through the user's body. The studies in [128] and [34] also presented the similar techniques. This electric profile transmitted during each touch to the device can be utilized to design a continuous and implicit authentication system that can differentiate one person from another with a high level of accuracy. Researchers have envisioned some application use cases for continuous authentication, such as personalizing applications to users in real time and displaying confidential data only when legitimate users are touching the surface. *"SkullConduct"* [132] is another example that leverages frequency characteristics of the audio signal as it travels through the head of the user. As the bone conduction speaker (that enables the audio signal to travel through the head) and microphone are readily available in wearable glasses such as Google Glass, the speaker can be used to create a sound that travels through the user's head, while the microphone can be used to record the audio signal. The changes in the recorded audio indicate the unique features of the user's head that are used to authenticate the user. Although seemingly viable, further work might be needed to evaluate the security and usability of this approach.

(3) *Hybrid Authentication:* Techniques underlying the hybrid authentication schemes combine widely used explicit authentication that establishes an initial identity (e.g., when the device is turned on) and implicit authentication that promptly and transparently de-authenticates the user by performing continuous reauthentication. For instance, Ojala et al. [109] presented a hybrid authentication system utilizing physiological sensors embedded in a wristband. Initial authentication is established through explicit fingerprint entry and the user is continuously authenticated through monitoring a set of vital signs (skin temperature, heart rate, skin capacitance, and motion) through a wrist-worn device. Thus, it combines the strength of an explicit biometric method with an unobtrusive and implicit continuous authentication method. Similarly, *Nymi* has developed a (~$150) wristband that offers hybrid authentication [108]. The *Nymi Band* requires the user to first create a biometric template that is stored locally for future instances of authentication. Thereafter, the user needs to authenticate to the Nymi Band only once to put it into an active state, using the secure explicit biometric modality (Nymi's HeartID, Apple's Touch ID, or other

modalities). Once authenticated, the Nymi Band will securely and continuously relay the device's authenticated credentials to provisioned terminals or services wirelessly using a secure Bluetooth or NFC connection. Thus, the users will remain authenticated as long as wristbands remain on the user's wrist or are not deactivated. Moreover, the provisioned services will not recognize a Nymi Band unless it is in an authenticated state or in an active state.

4.1.3 Wearable Possession-Based Authentication. This class of authentication scheme is also referred as token-based authentication, which is based on *what the user has*, such as memory cards or smart card tokens. Though the underlying techniques of token-based authentication can be sophisticated, it demands minimal user interaction, and only the user who possesses the token can open the associated locks. *Wearable Security Service [4]* conceptually resembles the physical tokens. The scheme requires the user to wear a smartwatch containing a certificate (key) issued and signed by a trusted *Certificate Authority* to authenticate against external devices/services (lock). The user places the watch against the authenticating terminal, and the watch transmits the certificate to the terminal through an IR link. The terminal examines the certificate to authenticate the user. "*Sound-Proof*" [80] is another token-based authentication system that does not require any interaction between the user and the authentication token (implemented on the phone). The scheme is based on the audio proximity between the user's phone and the terminal, which is determined by correlating the ambient sound recorded by the phone and the terminal. Instead of a phone, *Sound-Proof* can be implemented with a smartwatch as the second factor. Since the smartwatch is attached to the wrist of the user, the smartwatch and the terminal will be in very close proximity, which may help improve the efficiency and accuracy of the *Sound-Proof* system. In these schemes, frequent accesses to the terminal require frequent authentications, which in turn require frequent transmission and examination of certificate or audio pairs—a laborious task that reduces the usability and deployability of the system.

To address this issue, Corner and Nobel [35, 36] proposed *"Zero-Interaction Authentication (ZIA),"* a continuous authentication scheme, where a user wears a small authentication token (e.g., wristwatch) containing user credentials (key). The token can communicate with an authentication terminal through a short-range wireless link. Initially, the token is bound securely with the laptop through PIN authentication. After that, the terminal autonomously pulls a decryption key from the token whenever necessary without any user participation. Later, researchers presented a more effective and optimized variation of this approach. Sun et al. Sun et al. [142] proposed an optimized version of *ZIA* that incorporates careful key management and prudent communication schemes, while preserving the same security characteristics. Cha et al. [28] anticipated a secure two-factor authentication system using the combination of a smartwatch and mobile phone. In their authentication system, the user is authenticated for an online transaction on the phone as long as an NFC-enabled smartwatch remained nearby and coupled with the mobile phone.

With the same underlying notion (*ZIA*), researchers have also been exploring various other channels for secure device pairing, user identification, and data transmission. For instance, *"Wearable Key"* [103] is based on the transmission of signals through a user's body. *Wearable Key* consists of a key to be worn by the user for storing the user's credentials. *Wearable Key* broadcasts the user ID and credentials through the user's body using near-field technology, *TouchNet*, to the keyhole (receiver) that the user must touch. The system recognizes and authenticates the user based on received digital information. Roth et al. [124] presented a simple and continuous authentication system to authenticate a user to a multi-touch-enabled device based on the infrared-emitting ring. When a user wearing the ring touches the devices, the identity of the user is automatically transmitted in the form of infrared signals to the device and the user is identified and

authenticated. Laput et al. Laput et al. [90] proposed *"EMSense,"* a recognition system for electrical and electromechanical systems, built on the wrist-worn device. *EMSense* relies on the fact that the electrical system continuously emits low-magnitude electromagnetic noise. When the user touches the electrical system, *EMSense* senses emitted EM noise and can identify the unique signal from a set of pretrained objects. The authors envisioned an authentication system based on simply touching their devices employing a similar approach. The *"Loud and Clear" (L&C)* system proposed in [61] uses an audio channel to securely pair two devices. Thus, researchers have employed various channels including the user's body; infrared, electromagnetic noise; and audio to achieve a secure device pairing and user authentication.

4.2 User Safety

Today's wearable devices are incorporated with a wide range of sensors including physiological, inertial, and audio-visual sensors. By leveraging the signals captured by such sensors, various user safety schemes can be designed. For instance, motion sensors can be leveraged to design a pedestrian risk identification system [76]. An efficient driver drowsiness detection system can also be designed by leveraging various physiological sensors [93, 151].

4.2.1 Pedestrian Risk Identification System. The work of Jain et al. [76] reported a pedestrian safety scheme based on embedded inertial sensors, in particular an accelerometer, on a *wearable shoe* that alerts pedestrians before crossing the street. Monitoring the user's walking pattern based on the signals from inertial sensors, the application can accurately determine transitions between sidewalks and streets. It can also identify the pedestrian risks and generate an alert message to users when they step into the street. The presented application is not just limited to pedestrian safety; rather, it can also be employed in various other safety applications. For instance, it can be used in a driver-pedestrian awareness system, where each of the vehicles in the network announces its position to the other nearby vehicles and pedestrian applications. When a pedestrian is on the verge of stepping into the street, the application can alert either the vehicle's driver or the pedestrian for safety purposes. Also, if it is detected that the pedestrian is crossing the street, the application can delay the most distracting notifications on the phone, such as an SMS message or other notifications, for pedestrian safety. Further, by analyzing the historical walking patterns, it can guide pedestrians to follow good crossing or walking habits.

4.2.2 Driver Drowsiness Detection System. With the release of recent wireless wearables with bio-sensors, it is now possible to design reliable, efficient, and nonintrusive driver drowsiness detection systems. Due to drowsy driving, more than 100,000 crashes occur annually. Such systems can prevent or reduce such accidents. The work presented in [93] proposed a driver's safety scheme, in particular a driver drowsiness detection system, that detects the level of drowsiness and warns the driver before a mishap may happen. This safety scheme leverages the bio-sensors incorporated in the Bluetooth-enabled EEG headband for logging drivers' EEG signal and the smartwatch for analyzing the EEG signal, and creates alerts for drivers as per detection of the level of drowsiness. Leveraging a bio-sensor BioHarness 3 from Zephyr Technology, another preliminary work [151] has shown that drivers' breathing rate and heart rate can also be applied to detect the drowsiness level. In general, this application of wearable technology can lead to the development of products that can save many lives and avoid many accidents on the road. Beyond the driving scenario, these schemes can be applied to any critical situation where people should not fall asleep while executing a task (e.g., in mission-critical fields such as battlefields, machine operation, or mining).

4.2.3 Other Safety and Monitoring Applications. Beyond the two aforementioned applications, wearables can also be employed for personal safety purposes. Walking alone in unfamiliar, potentially unsafe places or in the middle of the night can be dangerous and scary, especially for women. Wearables like *Safelet*[43] can make users feel as if they are accompanied by someone all the time. These wearables might not prevent a potential attack per se but could notify friends, family, and law enforcement officials when the user might be in a dangerous situation. Wearables can also be used to keep an eye on pets by tracking the pets' location in real time using *Whistle GPS Pet Tracker.*[44]

5 CONCLUSIONS AND FUTURE DIRECTIONS

Wearable computing has been getting deployed in many personal, medical, and commercial domains. The availability of a wide range of sensors on wearable devices, such as physiological sensors, motion-position sensors, and audio-visual sensors, has facilitated numerous exciting applications in various aspects of life. However, as most of the wearables remain almost constantly attached to the body of the wearer, they have also raised unique security and privacy vulnerabilities. Wearables pose various security and privacy threats, such as unfettered access, sensor sniffing and side-channel attacks, wearers' and bystanders' privacy risks, and information leakage through social media and other channels. These threats have raised the demand for the design and implementation of appropriate defense mechanisms on wearable devices to mitigate, if not eliminate, the risks due to the existence of such threats. While wearables introduce new security and privacy vulnerabilities, they also promise to improve the existing security, privacy, and safety paradigms in unique ways while preserving the system's usability, especially in the context of authentication and user safety. In this research survey, we provided a detailed three-pronged investigation of the security and privacy of wearable computing, including a study of the primary threats and the associated defenses proposed in the research literature, as well as an exploration of the use of wearable computing to advance the security and privacy of other computing systems.

Our work identifies several future research directions focusing on the security and privacy of wearable devices. Major future research directions can be categorized as follows:

- *Lightweight usable authentication:* Due to the lack of a convenient authentication system on wearable devices, unauthorized entities can easily retrieve sensitive information captured by, and stored on, the device. Increasing use of such devices, therefore, motivates high demand for a lightweight and efficient authentication and identification mechanism for wearables. As these devices incorporate a wide range of sensors, these sensors can be leveraged for authentication and identification purposes. For instance, biometric authentication based on brainwave signals if EEG sensors are available, heart rhythm if heart rate sensors are available, and fingerprints or gestures and combinations thereof can be employed on the wearables. However, as these devices are typically resource constrained, they introduce challenges in designing efficient and effective authentication algorithms. Consequently, a study of the design and implementation of such authentication techniques and evaluation of their efficiency and usability in different types of wearable environments are highly needed in future work.
- *Zero-effort (de)authentication:* The availability of a wide range of sensors on wearables has also made it possible to design "zero effort" authentication/de-authentication systems. The

[43] Safelet – http://www.safelet.com/.
[44] Whistle GPS Pet Tracker for dogs and cats – http://www.pettracker.com/.

demand of such (de)authentication has been raised due to a widespread use of computing devices in day-to-day life. An attempt has been made to design such a system using a bracelet embedded with motion sensors [101], but a recent study [74] has shown that this scheme contains a design flaw that makes it vulnerable to a viable attack. Thus, though zero-effort (de)authentication is a compelling paradigm, the design and evaluation of such systems is a challenging task and need to be pursued with utmost care. Further research is necessary to explore this direction.

- *Defenses against side-channel attacks:* Motion-position sensors, such as accelerometers and gyroscopes, are considered nonsensitive resources by the current mobile operating systems, especially Android. By leveraging such sensors on a smartphone, malicious apps can surreptitiously infer the sensitive touch input, such as PIN, password, or credit card information, provided by the users. Being attached to the wearer's body, wearables, such as smartwatches, seem even more vulnerable to such motion-based side-channel attacks, as shown in recent research. How to defend against such attacks while preserving the usability offered by wearable devices is an interesting problem for future work.
- *Privacy -preserving schemes for cloud-services:* Several wearables often upload or synchronize their data to the online (cloud) service providers for their proper functionality or several other benefits. Since this data may contain sensitive information about the users and their surroundings, data should be stored securely by the providers in encrypted form. Though several privacy-preserving querying and computing schemes have been presented, only a few are designed for resource-constrained devices like wearables. So, designing optimized privacy-preserving schemes over encrypted data considering resource-constrained devices is a challenging task, and a further study is needed in this direction.
- *Safety risks, threats, underhanded benefits:* Many safety applications can also be built leveraging the sensors available on wearable devices, such as those geared for driver drowsiness detection, pedestrian safety, and UV exposure protection. However, the use of such devices can also introduce safety risks to the wearer in various scenarios such as while driving or crossing streets. Further, since many of the wearable devices are connected directly to social media or to cloud services, they also pose a threat of inadvertent sharing of sensitive information collected by the devices. Moreover, in many environments, wearables have a great potential to offer underhanded benefits to the wearer, such as in exams or casinos. Thorough studies are therefore needed to investigate the impact of wearable devices in all of these settings. Rigorous future investigation is required to design, implement, and evaluate the legal policies or software-based mechanisms to minimize the safety risks, threats, or underhanded benefits associated with wearable devices.
- *Secure and lightweight remote attestation:* Device integrity is a crucial security requirement of wearable devices. None of the security schemes implemented on the wearables would function properly without the assurance of the integrity of the device. Though several remote attestation mechanisms have been proposed in the literature for device integrity checking and verification, only a few are tailored toward resource-constrained devices like wearables. Therefore, future work is needed to design a secure and lightweight device integrity checking and verification mechanism geared for wearables.

APPENDIX

Table 5. Brief Description of Each of the Usability, Deployability, and Security Parameters as Used in [89] for Comparing PET Schemes

	Properties	Brief Description
Usability	User-Initiated	PETs require user to perform a certain action to mediate privacy preferences.
	Smartphone-Used	PETs leverage smartphone to relay privacy preferences.
	Dedicated-Device-Required	PETs require the user to carry a dedicated device.
	Physical-Artifact-Required	PETs require a user to carry or wear one-to-many physical artifact.
	Behavioral-Impact	PETs have a significant impact on user behavior.
Deployability	Negligible-Cost-per-User	Total cost per user including the costs at bystander's end and the cost at wearer's end while deploying a PET scheme is negligible.
	Accessibility	PETs function properly regardless of physical or mental disabilities.
	Requires-Device-to-Comply	Wearable cameras need to be updated accordingly (in terms of hardware and/or software) to deploy a PET scheme.
	Internet-Connection-Required	PETs need Internet connection tooperate properly.
Security	Third-Party-Service-Required	PETs rely on a third-party service to operate, which is assumed to be completely trustworthy.
	Anonymity	User's identity is not revealed during the operation of PET scheme.
	Visibility	Privacy preferences of the user get revealed as a result of PET requirement for the user to carry a dedicated device or wear physical artifact.

REFERENCES

[1] Zaid Ameen Abduljabbar, Hai Jin, Ayad Ibrahim, Zaid Alaa Hussien, Mohammed Abdulridha Hussain, Salah H. Abbdal, and Deqing Zou. 2016. Privacy-preserving image retrieval in IoT-cloud. In *Proceedings of the 2016 IEEE Trustcom/BigDataSE/I SPA*. IEEE, 799–806.

[2] Paarijaat Aditya, Rijurekha Sen, Peter Druschel, Seong Joon Oh, Rodrigo Benenson, Mario Fritz, Bernt Schiele, Bobby Bhattacharjee, and Tong Tong Wu. 2016. I-pic: A platform for privacy-compliant image capture. In *Proceedings of the 14th Annual International Conference on Mobile Systems, Applications, and Services (MobiSys'16)*, Vol. 16.

[3] Rakesh Agrawal and Ramakrishnan Srikant. 2000. Privacy-preserving data mining. In *ACM Sigmod Record*, Vol. 29. ACM, 439–450.

[4] Jalal Al-Muhtadi, Dennis Mickunas, and Roy Campbell. 2001. Wearable security services. In *Proceedings of the 2001 International Conference on Distributed Computing Systems Workshop*. IEEE, 266–271.

[5] Petar S. Aleksic and Aggelos K. Katsaggelos. 2006. Audio-visual biometrics. *Proc. IEEE* 94, 11 (2006), 2025–2044.

[6] Kamran Ali, Alex X. Liu, Wei Wang, and Muhammad Shahzad. 2015. Keystroke recognition using wifi signals. In *Proceedings of the 21st Annual International Conference on Mobile Computing and Networking*. ACM, 90–102.

[7] S. Abhishek Anand and Nitesh Saxena. 2016. A sound for a sound: Mitigating acoustic side channel attacks on password keystrokes with active sounds. *Financial Cryptography and Data Security*. Springer, 346–364.

[8] S. Abhishek Anand, Prakash Shrestha, and Nitesh Saxena. 2015. Bad sounds good sounds: Attacking and defending tap-based rhythmic passwords using acoustic signals. In *Cryptology and Network Security*. Springer, 95–110.

[9] William A. Arbaugh, David J. Farber, and Jonathan M. Smith. 1997. A secure and reliable bootstrap architecture. In *Proceedings of the 1997 IEEE Symposium on Security and Privacy*. IEEE, 65–71.

[10] Corey Ashby, Amit Bhatia, Francesco Tenore, and Jacob Vogelstein. 2011. Low-cost electroencephalogram (eeg) based authentication. In *Proceedings of the 2011 5th International IEEE/EMBS Conference on Neural Engineering (NER'11)*. IEEE, 442–445.

[11] Ashwin Ashok, Viet Nguyen, Marco Gruteser, Narayan Mandayam, Wenjia Yuan, and Kristin Dana. 2014. Do not share! Invisible light beacons for signaling preferences to privacy-respecting cameras. In *Proceedings of the 1st ACM MobiCom Workshop on Visible Light Communication Systems*. ACM, 39–44.

[12] Dmitri Asonov and Rakesh Agrawal. 2004. Keyboard acoustic emanations. In *Proceedings of the IEEE Symposium on Security and Privacy*. IEEE, 3.

[13] Adam J. Aviv, Katherine Gibson, Evan Mossop, Matt Blaze, and Jonathan M. Smith. 2010. Smudge attacks on smartphone touch screens. *WOOT* 10 (2010), 1–7.

[14] Daniel V. Bailey, Markus Dürmuth, and Christof Paar. 2014. Typing passwords with voice recognitio: How to authenticate to Google glass. In *Proceedings of the Symposium on Usable Privacy and Security*.

[15] Davide Balzarotti, Marco Cova, and Giovanni Vigna. 2008. Clearshot: Eavesdropping on keyboard input from video. In *Proceedings of the IEEE Symposium on Security and Privacy, 2008 (SP'08)*. IEEE, 170–183.
[16] Mukhtaj S. Barhm, Nidal Qwasmi, Faisal Z. Qureshi, and Khalil El-Khatib. 2011. Negotiating privacy preferences in video surveillance systems. In *Modern Approaches in Applied Intelligence*. Springer, 511–521.
[17] Andrea Bianchi and Ian Oakley. 2016. Wearable authentication: Trends and opportunities. *Inf. Technol.* 58, 5 (2016), 255–262.
[18] Dan Boneh, Craig Gentry, Shai Halevi, Frank Wang, and David J. Wu. 2013. Private database queries using somewhat homomorphic encryption. In *Proceedings of the International Conference on Applied Cryptography and Network Security*. Springer, 102–118.
[19] Joseph Bonneau, Cormac Herley, Paul C. Van Oorschot, and Frank Stajano. 2012. The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. In *Proceedings of the 2012 IEEE Symposium on Security and Privacy*. IEEE, 553–567.
[20] Raphael Bost, Raluca Ada Popa, Stephen Tu, and Shafi Goldwasser. 2015. Machine learning classification over encrypted data. *The Network and Distributed System Security*.
[21] Ferdinand Brasser, Brahim El Mahjoub, Ahmad-Reza Sadeghi, Christian Wachsmann, and Patrick Koeberl. 2015. TyTAN: Tiny trust anchor for tiny devices. In *Proceedings of the 2015 52nd ACM/EDAC/IEEE Design Automation Conference (DAC'15)*. IEEE, 1–6.
[22] Jack Brassil. 2005. Using mobile communications to assert privacy from video surveillance. In *19th IEEE International Parallel and Distributed Processing Symposium*. IEEE, 8–pp.
[23] Karel A. Brookhuis, Gerbrand de Vries, and Dick de Waard. 1991. The effects of mobile telephoning on driving performance. *Accident Anal. Prevent.* 23, 4 (1991), 309–316.
[24] Rondell Burge and Alex Chaparro. 2012. The effects of texting and driving on hazard perception. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, Vol. 56. Sage Publications, 715–719.
[25] Mario Čagalj, Srdjan Čapkun, and Jean-Pierre Hubaux. 2006. Key agreement in peer-to-peer wireless networks. *Proc. IEEE* 94, 2 (2006), 467–478.
[26] Kelly E. Caine. 2009. Supporting privacy by preventing misclosure. In *CHI'09 Extended Abstracts on Human Factors in Computing Systems*. ACM, 3145–3148.
[27] Cammozzo. 2016. Wearing or displaying a tagmenot means don't post my image unless face and personal details are blurred. Retrieved from http://tagmenot.info/.
[28] Byung-Rae Cha, Sang-Hun Lee, Soo-Bong Park, and Gun-Ki Lee4 Yoo-Kang Ji. 2015. Design of micro-payment to strengthen security by 2 factor authentication with mobile & wearable devices. *Advanced Science and Technology Letters* 109 (2015), 28–32.
[29] Pan Chan, Tzipora Halevi, and Nasir Memon. 2015. Glass OTP: Secure and convenient user authentication on google glass. In *Financial Cryptography and Data Security*. Springer, 298–308.
[30] Shoude Chang, Kirill V. Larin, Youxin Mao, Costel Flueraru, and Wahab Almuhtadi. 2011. Fingerprint spoof detection using near infrared optical analysis. In *State of the Art in Biometrics*, 57–84.
[31] Jagmohan Chauhan, Hassan Jameel Asghar, Anirban Mahanti, and Mohamed Ali Kaafar. 2016. Gesture-based continuous authentication for wearable devices: The smart glasses use case. In *Proceedings of the International Conference on Applied Cryptography and Network Security*. Springer, 648–665.
[32] Bo Cheng, Li Zhuo, Yu Bai, Yuanfan Peng, and Jing Zhang. 2014. Secure index construction for privacy-preserving large-scale image retrieval. In *Proceedings of the 2014 IEEE Fourth International Conference on Big Data and Cloud Computing (BdCloud'14)*. IEEE, 116–120.
[33] John Chuang, Hamilton Nguyen, Charles Wang, and Benjamin Johnson. 2013. I think, therefore I am: Usability and security of authentication using brainwaves. In *Financial Cryptography and Data Security*. Springer, 1–16.
[34] Cory Cornelius, Ronald Peterson, Joseph Skinner, Ryan Halter, and David Kotz. 2014. A wearable system that knows who wears it. In *Proceedings of the 12th Annual International Conference on Mobile Systems, Applications, and Services*. ACM, 55–67.
[35] Mark D. Corner and Brian D. Noble. 2002. Zero-interaction authentication. In *Proceedings of the 8th Annual International Conference on Mobile Computing and Networking*. ACM, 1–11.
[36] Mark D. Corner and Brian D. Noble. 2005. Protecting file systems with transient authentication. *Wireless Netw.* 11, 1–2 (2005), 7–19.
[37] Fanny Coudert, Denis Butin, and Daniel Le Métayer. 2015. Body-worn cameras for police accountability: Opportunities and risks. *Comput. Law Security Rev.* 31, 6 (2015), 749–762.
[38] Lawrence H. Cox. 1980. Suppression methodology and statistical disclosure control. *J. Amer. Statist. Assoc.* 75, 370 (1980), 377–385.
[39] Adrian Dabrowski, Edgar R. Weippl, and Isao Echizen. 2013. Framework based on privacy policy hiding for preventing unauthorized face image processing. In *2013 IEEE International Conference on Systems, Man, and Cybernetics (SMC'13)*. IEEE, 455–461.

[40] John Daugman. 2004. Iris recognition border-crossing system in the UAE. *Int. Airport Rev.* 8, 2 (2004).
[41] Alexander De Luca, Marian Harbach, Emanuel von Zezschwitz, Max-Emanuel Maurer, Bernhard Ewald Slawik, Heinrich Hussmann, and Matthew Smith. 2014. Now you see me, now you don't: Protecting smartphone authentication from shoulder surfers. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, 2937–2946.
[42] Dorothy E. Denning, Peter J. Denning, and Mayer D. Schwartz. 1979. The tracker: A threat to statistical database security. *ACM Trans. Database Syst. (TODS)* 4, 1 (1979), 76–96.
[43] Tamara Denning, Zakariya Dehlawi, and Tadayoshi Kohno. 2014. In situ with bystanders of augmented reality glasses: Perspectives on recording and privacy-mediating technologies. In *Proceedings of the 32nd Annual ACM Conference on Human Factors in Computing Systems*. ACM, 2377–2386.
[44] Mike DiGiovanni. 2013. GitHub – kaze0/bulletproof. Retrieved from https://github.com/kaze0/bulletproof.
[45] Frank A. Drews, Hina Yazdani, Celeste N. Godfrey, Joel M. Cooper, and David L. Strayer. 2009. Text messaging during simulated driving. *Human Factors* 51, 5 (2009), 762–770.
[46] Wenliang Du, Yunghsiang S. Han, and Shigang Chen. 2004. Privacy-preserving multivariate statistical analysis: Linear regression and classification. In *Proceedings of the 2004 SIAM International Conference on Data Mining*. SIAM, 222–233.
[47] Cynthia Dwork. 2006. Differential privacy. In *Proceedings of the 33rd International Colloquium on Automata, Languages and Programming, part II (ICALP'06)*. Vol. 4052. 1–12. https://www.microsoft.com/en-us/research/publication/differential-privacy/.
[48] Karim Eldefrawy, Gene Tsudik, Aurélien Francillon, and Daniele Perito. 2012. SMART: Secure and minimal architecture for (Establishing Dynamic) root of trust. In *NDSS*, Vol. 12. 1–15.
[49] Eurotech. 2013. Eurotech Group: Industrial computers and embedded boards for rugged system solutions - high performance computing. Retrieved from http://www.zypad.com/zypad/.
[50] Alexandre Evfimievski and Tyrone Grandison. 2009. Privacy preserving data mining. *IGI Global* (2009), 1–8.
[51] Bernardo Ferreira, Joao Rodrigues, Joao Leitao, and Henrique Domingos. 2015. Privacy-preserving content-based image retrieval in the cloud. In *Proceedings of the 2015 IEEE 34th Symposium on Reliable Distributed Systems (SRDS'15)*. IEEE, 11–20.
[52] Aurélien Francillon, Quan Nguyen, Kasper B. Rasmussen, and Gene Tsudik. 2014. A minimalist approach to remote attestation. In *Proceedings of the Conference on Design, Automation & Test in Europe*. European Design and Automation Association, 244.
[53] Davrondzhon Gafurov, Patrick Bours, and Einar Snekkenes. 2011. User authentication based on foot motion. *Signal Image Video Process.* 5, 4 (2011), 457–467.
[54] Davrondzhon Gafurov, Kirsi Helkala, and Torkjel Søndrol. 2006. Biometric gait authentication using accelerometer sensor. *J. Comput.* 1, 7 (2006), 51–59.
[55] Davrondzhon Gafurov, Einar Snekkenes, and Patrick Bours. 2007. Gait authentication and identification using wearable accelerometer sensor. In *Proceedings of the 2007 IEEE Workshop on Automatic Identification Advanced Technologies*. IEEE, 220–225.
[56] Davrondzhon Gafurov, Einar Snekkenes, and Patrick Bours. 2007. Spoof attacks on gait authentication system. *IEEE Trans. Inf. Forensics Security* 2, 3 (2007), 491–502.
[57] Davrondzhon Gafurov and Einar Snekkkenes. 2008. Arm swing as a weak biometric for unobtrusive user authentication. In Proceedings of the *International Conference on Intelligent Information Hiding and Multimedia Signal Processing, 2008 (IIHMSP'08)*. IEEE, 1080–1087.
[58] Christian Gehrmann, Chris J. Mitchell, and Kaisa Nyberg. 2004. Manual authentication for wireless devices. *RSA Cryptobytes* 7, 1 (2004), 29–37.
[59] Wayne C. W. Giang, Liberty Hoekstra-Atwood, and Birsen Donmez. 2014. Driver engagement in notifications a comparison of visual-manual interaction between smartwatches and smartphones. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, Vol. 58. Sage Publications, 2161–2165.
[60] Wayne C. W. Giang, Inas Shanti, Huei-Yen Winnie Chen, Alex Zhou, and Birsen Donmez. 2015. Smartwatches vs. smartphones: A preliminary report of driver behavior and perceived risk while responding to notifications. In *Proceedings of the 7th International Conference on Automotive User Interfaces and Interactive Vehicular Applications*. ACM, 154–161.
[61] Michael T. Goodrich, Michael Sirivianos, John Solis, Gene Tsudik, and Ersin Uzun. 2006. Loud and clear: Human-verifiable authentication based on audio. In *Proceedings of the 26th IEEE International Conference on Distributed Computing Systems (ICDCS'06)*. IEEE, 10–10.
[62] Google. 2016. Screen lock – Google Glass Help. Retrieved from https://support.google.com/glass/answer/4389349?hl=en.

[63] Marco Gruteser and Dirk Grunwald. 2004. A methodological assessment of location privacy risks in wireless hotspot networks. In *Security in Pervasive Computing*. Springer, 10–24.
[64] Tzipora Halevi and Nitesh Saxena. 2012. A closer look at keyboard acoustic emanations: Random passwords, typing styles and decoding techniques. In *Proceedings of the 7th ACM Symposium on Information, Computer and Communications Security*. ACM, 89–90.
[65] Adam Harvey. 2010. CV Dazzle: Camouflage from Face Detection. Retrieved from https://cvdazzle.com/.
[66] Jibo He, Alex Chaparro, B. Nguyen, Rondell J. Burge, Joseph Crandall, B. Chaparro, Rui Ni, and S. Cao. 2014. Texting while driving: Is speech-based text entry less risky than handheld text entry? *Accident Anal. Prevent.* 72 (2014), 287–295.
[67] Jibo He, Jake Ellis, William Choi, and Pingfeng Wang. 2015. Driving while reading using Google glass versus using a smart phone: Which is more distracting to driving performance? In *Proceedings of the 8th International Driving Symposium on Human Factors in Driver Assessment, Training and Vehicle Design*. 281–287.
[68] Benjamin Henne, Christian Szongott, and Matthew Smith. 2013. SnapMe if you can: Privacy threats of other peoples' geo-tagged media and what we can do about it. In *Proceedings of the 6th ACM Conference on Security and Privacy in Wireless and Mobile Networks*. ACM, 95–106.
[69] Steve Hodges, Lyndsay Williams, Emma Berry, Shahram Izadi, James Srinivasan, Alex Butler, Gavin Smyth, Narinder Kapur, and Ken Wood. 2006. SenseCam: A retrospective memory aid. In *Ubiquitous Computing (UbiComp'06)*. Springer, 177–193.
[70] Jaap-Henk Hoepman. 2004. The ephemeral pairing problem. In *Financial Cryptography*. Springer, 212–226.
[71] Christian Holz and Marius Knaust. 2015. Biometric touch sensing: Seamlessly augmenting each touch with continuous authentication. In *Proceedings of the 28th Annual ACM Symposium on User Interface Software & Technology*. ACM, 303–312.
[72] Roberto Hoyle, Robert Templeman, Steven Armes, Denise Anthony, David Crandall, and Apu Kapadia. 2014. Privacy behaviors of lifeloggers using wearable cameras. In *Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing*. ACM, 571–582.
[73] Chao-Yung Hsu, Chun-Shien Lu, and Soo-Chang Pei. 2012. Image feature extraction in encrypted domain with privacy-preserving SIFT. *IEEE Trans. Image Process.* 21, 11 (2012), 4593–4607.
[74] O. Huhta, P. Shrestha, S. Udar, M. Juuti, N. Saxena, and N. Asokan. 2016. Pitfalls in designing zero-effort deauthentication: Opportunistic human observation attacks. *The Network and Distributed System Security Symposium*.
[75] Yong Ho Hwang, Jae Woo Seo, and Il Joo Kim. 2014. Encrypted keyword search mechanism based on bitmap index for personal storage services. In *Proceedings of the 2014 IEEE 13th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom'14)*. IEEE, 140–147.
[76] Shubham Jain, Carlo Borgiattino, Yanzhi Ren, Marco Gruteser, Yingying Chen, and Carla Fabiana Chiasserini. 2015. Lookup: Enabling pedestrian safety services via shoe sensing. In *Proceedings of the 13th Annual International Conference on Mobile Systems, Applications, and Services*. ACM, 257–271.
[77] Markus Jakobsson and Susanne Wetzel. 2001. Security weaknesses in bluetooth. In *Topics in Cryptology (CT-RSA'01)*. Springer, 176–191.
[78] Benjamin Johnson, Thomas Maillart, and John Chuang. 2014. My thoughts are not your thoughts. In *Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct Publication*. ACM, 1329–1338.
[79] Ari Juels. 2006. RFID security and privacy: A research survey. *IEEE J. Selected Areas Commun.* 24, 2 (2006), 381–394.
[80] Nikolaos Karapanos, Claudio Marforio, Claudio Soriente, and Srdjan Capkun. 2015. Sound-proof: Usable two-factor authentication based on ambient sound. In *Proceedings of the 24th USENIX Security Symposium (USENIX Security'15)*. 483–498.
[81] Rick Kennell and Leah H. Jamieson. 2003. Establishing the genuinity of remote computer systems. In *USENIX Security*. 21.
[82] Rasib Khan, Ragib Hasan, and Jinfang Xu. 2015. SEPIA: Secure-PIN-authentication-as-a-service for ATM using mobile and wearable devices. In *Proceedings of the 2015 3rd IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud'15)*. IEEE, 41–50.
[83] Daniel V. Klein. 1990. Foiling the cracker: A survey of, and improvements to, password security. In *Proceedings of the 2nd USENIX Security Workshop*. 5–14.
[84] Patrick Koeberl, Steffen Schulz, Ahmad-Reza Sadeghi, and Vijay Varadharajan. 2014. TrustLite: A security architecture for tiny embedded devices. In *Proceedings of the 9th European Conference on Computer Systems*. ACM, 10.
[85] Tadayoshi Kohno, Joel Kollin, David Molnar, and Franziska Roesner. 2015. *Display Leakage and Transparent Wearable Displays: Investigation of Risk, Root Causes, and Defenses*. Technical Report MSR-TR-2015-18. Retrieved from http://research.microsoft.com/apps/pubs/default.aspx?id=240860.

[86] Joonho Kong, Farinaz Koushanfar, Praveen K. Pendyala, Ahmad-Reza Sadeghi, and Christian Wachsmann. 2014. PUFatt: Embedded platform attestation based on novel processor-based PUFs. In *Proceedings of the 51st Annual Design Automation Conference*. ACM, 1–6.

[87] Mohammed Korayem, Robert Templeman, Dennis Chen, David Crandall, and Apu Kapadia. 2014. Screenavoider: Protecting computer screens from ubiquitous cameras. *arXiv preprint arXiv:1412.0008* (2014).

[88] Xeno Kovah, Corey Kallenberg, Chris Weathers, Amy Herzog, Matthew Albin, and John Butterworth. 2012. New results for timing-based attestation. In *Proceedings of the 2012 IEEE Symposium on Security and Privacy (SP'12)*. IEEE, 239–253.

[89] Katharina Krombholz, Adrian Dabrowski, Matthew Smith, and Edgar Weippl. 2015. Ok glass, leave me alone: Towards a systematization of privacy enhancing technologies for wearable computing. In *Financial Cryptography and Data Security*. Springer, 274–280.

[90] Gierad Laput, Chouchang Yang, Robert Xiao, Alanson Sample, and Chris Harrison. 2015. Em-sense: Touch recognition of uninstrumented, electrical and electromechanical objects. In *Proceedings of the 28th Annual ACM Symposium on User Interface Software & Technology*. ACM, 157–166.

[91] Jeong Jun Lee, Seungin Noh, Kang Ryoung Park, and Jaihie Kim. 2004. Iris recognition in wearable computer. In *Biometric Authentication*. Springer, 475–483.

[92] Linda Lee, Serge Egelman, Joong Hwa Lee, and David Wagner. 2015. Risk perceptions for wearable devices. *arXiv preprint arXiv:1504.05694* (2015).

[93] Gang Li, Boon-Leng Lee, and Wan-Young Chung. 2015. Smartwatch-based wearable EEG system for driver drowsiness detection. *IEEE Sensors J.* 15, 12 (2015), 7169–7180.

[94] Mengyuan Li, Yan Meng, Junyi Liu, Haojin Zhu, Xiaohui Liang, Yao Liu, and Na Ruan. 2016. When CSI meets public WiFi: Inferring your mobile phone password via WiFi signals. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*. ACM, 1068–1079.

[95] Sugang Li, Ashwin Ashok, Yanyong Zhang, Chenren Xu, Janne Lindqvist, and Macro Gruteser. 2016. Whose move is it anyway? Authenticating smart wearable devices using unique head movement patterns. In *Proceedings of the 2016 IEEE International Conference on Pervasive Computing and Communications (PerCom'16)*. IEEE, 1–9.

[96] Yanlin Li, Jonathan M. McCune, and Adrian Perrig. 2011. VIPER: Verifying the integrity of PERipherals' firmware. In *Proceedings of the 18th ACM Conference on Computer and Communications Security*. ACM, 3–16.

[97] Xiangyu Liu, Zhe Zhou, Wenrui Diao, Zhou Li, and Kehuan Zhang. 2015. When good becomes evil: Keystroke inference with smartwatch. In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*. ACM, 1273–1285.

[98] Wenjun Lu, Avinash L. Varna, Ashwin Swaminathan, and Min Wu. 2009. Secure image retrieval through feature protection. In *Proceedings of the IEEE International Conference on Acoustics, Speech and Signal Processing, 2009 (ICASSP'09)*. IEEE, 1533–1536.

[99] Anindya Maiti, Murtuza Jadliwala, Jibo He, and Igor Bilogrevic. 2015. (Smart) watch your taps: Side-channel keystroke inference attacks using smartwatches. In *Proceedings of the 2015 ACM International Symposium on Wearable Computers*. ACM, 27–30.

[100] Sebastien Marcel and José R. Del Millan. 2007. Person authentication using brainwaves (EEG) and maximum a posteriori model adaptation. *IEEE Trans. Pattern Anal. Mach. Intell.* 29, 4 (2007), 743–752.

[101] Shrirang Mare, Andres Molina Markham, Cory Cornelius, Ronald Peterson, and David Kotz. 2014. Zebra: Zero-effort bilateral recurring authentication. In *Proceedings of the 2014 IEEE Symposium on Security and Privacy (SP'14)*. IEEE, 705–720.

[102] Ivan Martinovic, Doug Davies, Mario Frank, Daniele Perito, Tomas Ros, and Dawn Song. 2012. On the feasibility of side-channel attacks with brain-computer interfaces. In *Proceedings of the USENIX Security Symposium*. 143–158.

[103] Nobuyuki Matsushita, Shigeru Tajima, Yuji Ayatsuka, and Jun Rekimoto. 2000. Wearable key: Device for personalizing nearby environment. In *Proceedings of the 4th International Symposium on Wearable Computers*. IEEE, 119–126.

[104] Belden Menkus. 1988. Understanding the use of passwords. *Comput. Security* 7, 2 (1988), 132–136.

[105] Alex Migicovsky, Zakir Durumeric, Jeff Ringenberg, and J. Alex Halderman. 2014. Outsmarting proctors with smartwatches: A case study on wearable computing security. In *Financial Cryptography and Data Security*. Springer, 89–96.

[106] Emiliano Miluzzo, Alexander Varshavsky, Suhrid Balakrishnan, and Romit Roy Choudhury. 2012. Tapprints: Your finger taps have fingerprints. In *Proceedings of the 10th International Conference on Mobile Systems, Applications, and Services*. ACM, 323–336.

[107] Long Hoang Nguyen and Andrew William Roscoe. 2011. Authentication protocols based on low-bandwidth unspoofable channels: A comparative survey. *J. Comput. Security* 19, 1 (2011), 139–201.

[108] Nymi. 2014. Nymi | Convenient Authentication Anywhere. Retrieved from https://nymi.com/.

[109] Sampo Ojala, Jari Keinanen, and Jorma Skytta. 2008. Wearable authentication device for transparent login in nomadic applications environment. In *Proceedings of the 2nd International Conference on Signals, Circuits and Systems, 2008 (SCS'08)*. IEEE, 1–6.

[110] Emmanuel Owusu, Jun Han, Sauvik Das, Adrian Perrig, and Joy Zhang. 2012. ACCessory: Password inference using accelerometers on smartphones. In *Proceedings of the 12th Workshop on Mobile Computing Systems & Applications*. ACM, 9.

[111] Ramaswamy Palaniappan. 2006. Electroencephalogram signals from imagined activities: A novel biometric identifier for a small population. In *Intelligent Data Engineering and Automated Learning (IDEAL'06)*. Springer, 604–611.

[112] Ramaswamy Palaniappan. 2008. Two-stage biometric authentication method using thought activity brain waves. *Int. J. Neural Syst.* 18, 01 (2008), 59–66.

[113] Frank Pallas, Max-Robert Ulbricht, Lorena Jaume-Palasí, and Ulrike Höppner. 2014. Offlinetags: A novel privacy approach to online photo sharing. In *CHI'14 Extended Abstracts on Human Factors in Computing Systems*. ACM, 2179–2184.

[114] Bryan Parno, Jonathan M. McCune, and Adrian Perrig. 2010. Bootstrapping trust in commodity computers. In *Proceedings of the 2010 IEEE Symposium on Security and Privacy (SP'10)*. IEEE, 414–429.

[115] Shwetak N. Patel, Jay W. Summet, and Khai N. Truong. 2009. Blindspot: Creating capture-resistant spaces. In *Protecting Privacy in Video Surveillance*. Springer, 185–201.

[116] Greig Paul and James Irvine. 2014. Privacy implications of wearable health devices. In *Proceedings of the 7th International Conference on Security of Information and Networks*. ACM, 117.

[117] Raluca Ada Popa, Catherine Redfield, Nickolai Zeldovich, and Hari Balakrishnan. 2011. CryptDB: Protecting confidentiality with encrypted query processing. In *Proceedings of the 23rd ACM Symposium on Operating Systems Principles*. ACM, 85–100.

[118] Raluca Ada Popa, Emily Stark, Steven Valdez, Jonas Helfer, Nickolai Zeldovich, and Hari Balakrishnan. 2014. Building web applications on top of encrypted data using Mylar. In *NSDI*. 157–172.

[119] M. Poulos, M. Rangoussi, N. Alexandris, A. Evangelou, and others. 2002. Person identification from the EEG using nonlinear signal classification. *Methods Inf. Med.* 41, 1 (2002), 64–75.

[120] Mahmudur Rahman, Bogdan Carbunar, and Madhusudan Banik. 2013. Fit and vulnerable: Attacks and defenses for a health monitoring device. *arXiv preprint arXiv:1304.5672* (2013).

[121] Nisarg Raval, Animesh Srivastava, Ali Razeen, Kiron Lebeck, Ashwin Machanavajjhala, and Landon P. Cox. 2016. What you mark is what apps see. In *Proceedings of the ACM International Conference on Mobile Systems, Applications, and Services (Mobisys'16)*.

[122] Mehran Roshandel, Aarti Munjal, Peyman Moghadam, Shahin Tajik, and Hamed Ketabdar. 2014. Multi-sensor finger ring for authentication based on 3d signatures. In *Proceedings of the International Conference on Human-Computer Interaction*. Springer, 131–138.

[123] Volker Roth, Kai Richter, and Rene Freidinger. 2004. A PIN-entry method resilient against shoulder surfing. In *Proceedings of the 11th ACM Conference on Computer and Communications Security*. ACM, 236–245.

[124] Volker Roth, Philipp Schmidt, and Benjamin Güldenring. 2010. The IR ring: Authenticating users' touches on a multi-touch display. In *Proceedings of the 23nd Annual ACM Symposium on User Interface Software and Technology*. ACM, 259–262.

[125] Virginia Ruiz-Albacete, Pedro Tome-Gonzalez, Fernando Alonso-Fernandez, Javier Galbally, Julian Fierrez, and Javier Ortega-Garcia. 2008. Direct attacks using fake images in iris verification. In *Proceedings of the European Workshop on Biometrics and Identity Management*. Springer, 181–190.

[126] Young Sam Ryu, Do Hyong Koh, Brad L. Aday, Xavier A. Gutierrez, and John D. Platt. 2010. Usability evaluation of randomized keypad. *J. Usabil. Stud.* 5, 2 (2010), 65–75.

[127] Hasan Sajid and Sen-ching S. Cheung. 2015. VSig: Hand-gestured signature recognition and authentication with wearable camera. In *Proceedings of the 2015 IEEE International Workshop on Information Forensics and Security (WIFS'15)*. IEEE, 1–6.

[128] Munehiko Sato, Ivan Poupyrev, and Chris Harrison. 2012. Touché: Enhancing touch interaction on humans, screens, liquids, and everyday objects. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, 483–492.

[129] Ben D. Sawyer, Victor S. Finomore, Andres A. Calvo, and Peter A. Hancock. 2014. Google glass a driver distraction cause or cure? *Human Factors* 56, 7 (2014), 1307–1321.

[130] Jeremy Schiff, Marci Meingast, Deirdre K. Mulligan, Shankar Sastry, and Ken Goldberg. 2009. Respectful cameras: Detecting visual markers in real-time to address privacy concerns. In *Protecting Privacy in Video Surveillance*. Springer, 65–89.

[131] Roman Schlegel, Kehuan Zhang, Xiao-yong Zhou, Mehool Intwala, Apu Kapadia, and XiaoFeng Wang. 2011. Soundcomber: A stealthy and context-aware sound trojan for smartphones. In *NDSS*, Vol. 11. 17–33.

[132] Stefan Schneegass, Youssef Oualil, and Andreas Bulling. 2016. SkullConduct: Biometric user identification on eyewear computers using bone conduction through the skull. In *Proceedings of the 34th ACM SIGCHI Conference on Human Factors in Computing Systems (CHI'16)* (2016-01-01). IEEE.

[133] Steffen Schulz, Ahmad-Reza Sadeghi, and Christian Wachsmann. 2011. Short paper: Lightweight remote attestation using physical functions. In *Proceedings of the 4th ACM Conference on Wireless Network Security*. ACM, 109–114.

[134] Arvind Seshadri, Adrian Perrig, Leendert Van Doorn, and Pradeep Khosla. 2004. SWATT: Software-based attestation for embedded devices. In *Proceedings of the 2004 IEEE Symposium on Security and Privacy*. IEEE, 272–282.

[135] Hossein Shafagh, Anwar Hithnawi, Andreas Dröscher, Simon Duquennoy, and Wen Hu. 2015. Talos: Encrypted query processing for the internet of things. In *Proceedings of the 13th ACM Conference on Embedded Networked Sensor Systems*. ACM, 197–210.

[136] Yiran Shen, Chengwen Luo, Weitao Xu, and Wen Hu. 2015. Poster: An online approach for gait recognition on smart glasses. In *Proceedings of the 13th ACM Conference on Embedded Networked Sensor Systems*. ACM, 389–390.

[137] Kohei Shiraga, Ngo Thanh Trung, Ikuhisa Mitsugami, Yasuhiro Mukaigawa, and Yasushi Yagi. 2012. Gait-based person authentication by wearable cameras. In *Proceedings of the 2012 9th International Conference on Networked Sensing Systems (INSS'12)*. IEEE, 1–7.

[138] Jiayu Shu, Rui Zheng, and Pan Hui. 2016. Cardea: Context-aware visual privacy protection from pervasive cameras. *arXiv preprint arXiv:1610.00889* (2016).

[139] Diksha Shukla, Rajesh Kumar, Abdul Serwadda, and Vir V. Phoha. 2014. Beware, your hands reveal your secrets! In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*. ACM, 904–917.

[140] Dawn Xiaoding Song, David Wagner, and Adrian Perrig. 2000. Practical techniques for searches on encrypted data. In *Proceedings of the 2000 IEEE Symposium on Security and Privacy, 2000 (S&P'00)*. IEEE, 44–55.

[141] Yihang Song, Madhur Kukreti, Rahul Rawat, and Urs Hengartner. 2014. Two novel defenses against motion-based keystroke inference attacks. *arXiv preprint arXiv:1410.7746* (2014).

[142] Da-Zhi Sun, Jin-Peng Huai, Ji-Zhou Sun, Jia-Wan Zhang, and Zhi-Yong Feng. 2008. A new design of wearable token system for mobile device security. *IEEE Trans. Consumer Electron.* 54, 4 (2008), 1784–1789.

[143] Robert Templeman, Mohammed Korayem, David J. Crandall, and Apu Kapadia. 2014. PlaceAvoider: Steering first-person cameras away from sensitive spaces. In *NDSS*.

[144] Robert Templeman, Zahid Rahman, David Crandall, and Apu Kapadia. 2012. PlaceRaider: Virtual theft in physical spaces with smartphones. *arXiv preprint arXiv:1209.5982* (2012).

[145] Julie Thorpe, Paul C. van Oorschot, and Anil Somayaji. 2005. Pass-thoughts: Authenticating with our minds. In *Proceedings of the 2005 Workshop on New Security Paradigms*. ACM, 45–56.

[146] Jaideep Vaidya, Murat Kantarcıoğlu, and Chris Clifton. 2008. Privacy-preserving naive bayes classification. *VLDB J.* 17, 4 (2008), 879–898.

[147] Wouter Van Vlaenderen, Jens Brulmans, Jo Vermeulen, and Johannes Schöning. 2015. Watchme: A novel input method combining a smartwatch and bimanual interaction. In *Proceedings of the 33rd Annual ACM Conference Extended Abstracts on Human Factors in Computing Systems*. ACM, 2091–2095.

[148] Serge Vaudenay. 2005. Secure communications over insecure channels based on short authenticated strings. In *Advances in Cryptology (CRYPTO'05)*. Springer, 309–326.

[149] He Wang, Ted Tsung-Te Lai, and Romit Roy Choudhury. 2015. MoLe: Motion leaks through smartwatch sensors. In *Proceedings of the 21st Annual International Conference on Mobile Computing and Networking*. ACM, 155–166.

[150] Tianzi Wang, Zheng Song, Jian Ma, Yongping Xiong, and Yun Jie. 2013. An anti-fake iris authentication mechanism for smart glasses. In *Proceedings of the 2013 3rd International Conference on Consumer Electronics, Communications and Networks (CECNet'13)*. IEEE, 84–87.

[151] Brandy Warwick, Nicholas Symons, Xiao Chen, and Kaiqi Xiong. 2015. Detecting driver drowsiness using wireless wearables. In *Proceedings of the 2015 IEEE 12th International Conference on Mobile Ad Hoc and Sensor Systems (MASS'15)*. IEEE, 585–588.

[152] Christian Winkler, Jan Gugenheimer, Alexander De Luca, Gabriel Haas, Philipp Speidel, David Dobbelstein, and Enrico Rukzio. 2015. Glass unlock: Enhancing security of smartphone unlocking through leveraging a private near-eye display. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems, CHI*, Vol. 15. 1407–1410.

[153] Rebecca Wright and Zhiqiang Yang. 2004. Privacy-preserving Bayesian network structure computation on distributed heterogeneous data. In *Proceedings of the 10th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*. ACM, 713–718.

[154] Muchen Wu, Parth H. Pathak, and Prasant Mohapatra. 2015. Enabling privacy-preserving first-person cameras using low-power sensors. In *Proceedings of the 2015 12th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON'15)*. IEEE, 444–452.

[155] Zhihua Xia, Yi Zhu, Xingming Sun, Zhan Qin, and Kui Ren. 2015. Towards privacy-preserving content-based image retrieval in cloud computing. *IEEE Trans. Cloud Comput.* (2015).

[156] Zhi Xu, Kun Bai, and Sencun Zhu. 2012. Taplogger: Inferring user inputs on smartphone touchscreens using on-board motion sensors. In *Proceedings of the 5th ACM Conference on Security and Privacy in Wireless and Mobile Networks*. ACM, 113–124.

[157] Dhruv Kumar Yadav, Beatrice Ionascu, Sai Vamsi Krishna Ongole, Aditi Roy, and Nasir Memon. 2015. Design and analysis of shoulder surfing resistant PIN based authentication mechanisms on Google glass. In *Financial Cryptography and Data Security*. Springer, 281–297.

[158] Takayuki Yamada, Seiichi Gohshi, and Isao Echizen. 2013. Privacy visor: Method for preventing face image detection by using differences in human and device sensitivity. In *Communications and Multimedia Security*. Springer, 152–161.

[159] Junshuang Yang, Yanyan Li, and Mengjun Xie. 2015. MotionAuth: Motion-based authentication for wrist worn smart devices. In *Proceedings of the 2015 IEEE International Conference on Pervasive Computing and Communication Workshops (PerCom Workshops'15)*. IEEE, 550–555.

[160] Zhiqiang Yang, Sheng Zhong, and Rebecca N. Wright. 2005. Privacy-preserving classification of customer data without loss of accuracy. In *Proceedings of the 2005 SIAM International Conference on Data Mining*. SIAM, 92–102.

[161] Qinggang Yue, Zhen Ling, Xinwen Fu, Benyuan Liu, Wei Yu, and Wei Zhao. 2014. My Google glass sees your passwords! In *Black Hat USA 2014 White Paper*.

[162] Roberto Yus, Primal Pappachan, Prajit Kumar Das, Eduardo Mena, Anupam Joshi, and Tim Finin. 2014. FaceBlock: Privacy-aware pictures for google glass. In *Proceedings of the 12th Annual International Conference on Mobile Systems, Applications, and Services (MobiSys'14)*, Vol. 14. 1.

[163] Wei Zhou and Selwyn Piramuthu. 2014. Security/privacy of wearable fitness tracking IoT devices. In *Proceedings of the 2014 9th Iberian Conference on Information Systems and Technologies (CISTI'14)*. IEEE, 1–5.

[164] Li Zhuang, Feng Zhou, and J. Doug Tygar. 2009. Keyboard acoustic emanations revisited. *ACM Trans. Inf. Syst. Security (TISSEC)* 13, 1 (2009), 3.

Received March 2017; revised August 2017; accepted August 2017