Special Issue

Andrea Bianchi and Ian Oakley*

Wearable authentication: Trends and opportunities

DOI 10.1515/itit-2016-0010
Received February 18, 2016; accepted June 3, 2016

Abstract: Wearables are a rapidly emerging device category with wide-reaching use scenarios. The novel form factors and broad potential of this technology pose new security challenges: devices are typically *on and close* to a user. Furthermore, while they possess limited input and output channels, they often feature rich sensing, computing and communication capabilities. Due to this novel context, this paper argues that researchers need to reconsider the functional, technical and social aspects of authenticating, or securely establishing a user's identity, for wearable devices. This paper contributes to ongoing work on this topic by reviewing wearable authentication schemes according to the traditional classification of authentication via tokens, passwords or biometrics. The goal of this review is to provide an illustrated overview of key advances in the area over the past decade that covers a variety of form factors (wristbands, glasses, jewelry, etc) and modes of operation (single or multi-factor authentication, on one or multiple devices). Finally, we tie the review together by identifying four key themes that will drive future research: the raise of implicit authentication that requires no dedicated user action; the use of wearable devices for authentication in conjunction with other systems; the potential and richness of current available technology and tools for wearable devices and; the importance and challenges of maintaining privacy and security in wearable contexts.

Keywords: Wearable, authentication, passwords, tokens, biometrics.

ACM CCS: Security and privacy → Human and societal aspects of security and privacy → Usability in security and privacy

***Corresponding author: Ian Oakley,** Department of Human and System Engineering, UNIST, Ulsan, Republic of Korea, e-mail: ian.r.oakley@gmail.com
Andrea Bianchi: KAIST, Department of Industrial Design, Daejeon, Republic of Korea

1 Introduction

Wearable computing is a rapidly emerging device category encompassing a broad range of diverse form factors: from glasses, to wrist-bands, to jewelry. Current projections indicate the market for wearable devices will triple in the period from 2013 to 2018 [5] – many more of us will be wearing digital technology to achieve tasks such understanding our fitness and health (www.fitbit.com), accessing information [27], identifying ourselves to third party services [28], monitoring or tracking (e.g., http://snowfox.family) and to communicate with one another [43]. While wearable applications show considerable promise in terms of qualities such as accuracy, reliability and convenience, they also raise new questions in terms of security, authentication and privacy. This is because much of the value of the services offered by wearable devices rests on the confidential and personal nature of the information they capture, store, manipulate and transmit – data about the health, identity or communications of individuals. Furthermore, future wearable devices have also considerable promise as password managers and tokens that mediate access to users' diverse physical devices and online accounts. In order to prevent unauthorized access to data or use of these features, we argue that authentication to wearable devices will need become simple, rapid and secure and, ultimately, commonplace.

However, adapting established authentication techniques from other mobile or desktop scenarios to wearables can be challenging. This can be seen most strongly in the poor fit between wearable technologies and traditional authentication techniques based on the entry of secret information in the form of passwords or PINs. Quite simply, most wearable devices lack suitable input devices to support rapid, reliable and secure entry of textual or numerical data – many lack displays and expressive input surfaces or are simply too small to show the complex keypads or keyboards required for secure, high entropy passwords. We argue that the lack of traditional input/output mechanisms makes existing password authentication techniques at best laborious and at worst unsuitable for use in wearable contexts.

Despite this problem, wearable devices also provide promising new avenues for authenticating users and securing systems (see Figure 1 for examples). More so than other device categories, they can be designed to unobtrusively and continuously capture biometric data about their owners, potentially providing a high level of security with a minimum of user intervention. With technology that can detect when a device is donned or removed, it also becomes possible to authenticate a user when a device is put on and maintain a high level of confidence about the user's identity for a sustained period. A general trend is clear: wearables provide novel opportunities to improve or redesign approaches to authentication.

Taking advantage of these possibilities is particularly important given the application scenarios enabled by wearable technology. For example, in the domain of health, while current key application areas focus on tracking activity or vitals – sensitive data that needs be stored and transmitted securely – emerging and future scenarios involve systems that can perform interventions, such as implantable glucose regulation systems for diabetics. The security of such systems goes beyond issues of privacy to encompass the critical issues of safety and health – they have the ability to act on and influence the bodily state of their users. Similarly, a current wearable application in the area of tracking is child monitoring – a simple device worn by a minor broadcasts its location to a parent or guardian. While the objective is clearly to increase the safety and security of the child, the data stream itself represents highly sensitive information that a nefarious attacker could seek to compromise. As wearable devices are in close proximity to the body and readily available, we argue that they present new security scenarios that match poorly with the values and intentions inherent in traditional authentication systems such as passwords.

Reflecting these perspectives, this article provides a review of existing approaches, technologies and interfaces for wearable authentication. The contributions of this survey are to consolidate current research into a coherent framework, highlight common threads, understand threats and isolate promising avenues for future investigation.

2 Classification

Our review of wearable authentication systems is structured according to the established classification scheme, that separates authentication techniques into those that rely on tokens (something that you own), passwords (something that you know) and biometrics (something you are). The use of this traditional classification scheme provides two key benefits. First its wide use as a framework in the past, such as in the analysis of authentication for ubiquitous computing [42], enables ready reflection on the similarities and differences inherent in the wearable paradigm. Second, the use of a traditional framework also allows us to explore has the boundaries between its categories and highlight where they are beginning to fray. This exposes limitations in the current scheme and suggests new refinements that may better fit emerging approaches to authentication. Perhaps most prominently, this fraying results from the fact that many wearable authentication schemes involve hybrid approaches that span two or more of the traditional categories. Discussing and exploring those overlaps provides a useful way to understand underlying trends in wearable authentication and predict the future of the field.

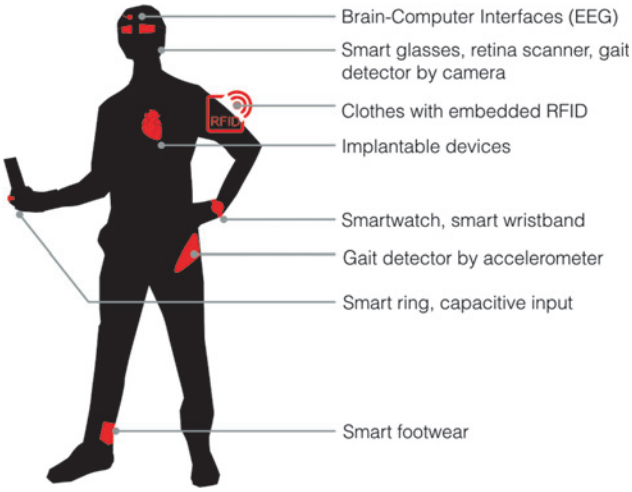

Figure 1: Authentication wearable interfaces (tokens, passwords, biometrics) with different form factors.

3 Wearable tokens

Physical keys are among the oldest form of access token – they restrict access to a private location to those in possession of a valid key [22]. They remain popular today. Although the underlying technology can be highly sophisticated [34], user interaction is minimal and transparent – only a person who physically possesses the key can open the matching lock. Keys can also be shared or duplicated to delegate access or manage access across a group of individuals. Furthermore, keys can take many physical forms and are highly portable; many are small enough to be worn clipped to the body or clothes. However, their main limitation lies in this same physicality – they must be carried

and therefore can be lost, stolen, or duplicated without authorization. Digital token implementations that mimic key functionality typically balance maintaining their positive qualities with addressing their weaknesses.

Systems that conceptually resemble physical keys and locks include Al-Muhtadi et al.'s [1] wearable security service. A user wears a smart-watch containing a trusted certificate (a key) and authenticates to a terminal (a lock) by placing the watch against it. The watch transmits the certificate to the terminal via an IR link and the terminal examines it to provide the authorized level of access. Repeated authentications require repeated transmissions – a laborious task if frequent access is required.

To address this issue, Corner and Noble [10] propose Zero-Interaction Authentication (ZIA), a paradigm in which a user wears an active authentication token capable of storing credentials and communicating with a laptop over a short-range wireless link. An initial PIN authentication is used to bind the token securely to the laptop. Subsequently, the laptop autonomously polls the token to acquire a decryption certificate whenever necessary and without further user intervention. Variations on this concept appear frequently: Sun et al. [44] propose a set of technical optimizations while Cha et al. [6] envision a broadly similar system using the combination of a smart-watch and mobile phone. In Cha's system a user is authenticated for secure online transactions on the phone so long as the NFC-enabled smart-watch remains nearby and coupled with the mobile device. Kurkovsky et al. [28] elaborate on this type of authentication, terming it *composite continuous authentication* and suggesting that it fundamentally involves a user logging in to some resource with a PIN or password and then having their ongoing presence continuously verified via the proximity of a unique token identifier such as an RFID tag. They consider the authentication composite because it relies on multiple authentication methods and continuous because the presence of the users is monitored after the initial login.

Further variations on this theme exploit side or hidden channels for pairing devices, identifying users or securely transmitting data. For example, the Wearable Key [32] relies on transmission of signals through the user's body [35]. In this system, a user wears a physical device that broadcasts their ID and credentials via an electrode in contact with their skin. If this signal reaches a predetermined keyhole, a receiver unit that the user must touch, the system recognizes and authenticates the user. EM-Sense [29], adapts the idea of using the body as hidden channel but applies it to a more general scenario. It again relies on a worn sensor in the form of a bracelet but leverages the fact that electrical devices continuously emit low magnitude electromagnetic noise. When a user touches a device, such as their laptop, the bracelet senses the EM noise this device produces and can identify its unique signal from a set of pre-trained objects. In this way, the authors envisage an authentication system based on simply touching different devices. In effect, a user's devices become their own access tokens. Wearable tokens have also been used to facilitate or maintain device pairings. Goodrich et al., [19], for example, propose a system that securely pairs two devices using an audio channel. Roth et al. [37] demonstrates a simple system based on infra-red emitting ring capable of authenticating to a tabletop device. Basically, when a user touches the tabletop wearing their ring, the IR ring identity is automatically transmitted to the table and the user is identified and authenticated.

Finally, wearable tokens have also been proposed as tools to mediate access to implantable medical devices such as cardiac defibrillators and pacemakers. Many such devices use wireless protocols to allow software modifications after implantation. However, due to the potential of patients' experiencing physical harm, such links are typically protected by strong passwords. In order to deal with situations in which the passwords are unavailable (for example, due to the patient being incapacitated), researchers have proposed various methods to make them available to medical staff. Perhaps the simplest idea is simply to have them written on physical tokens carried by the patients [12]. Alternative token designs including visible tattoos, ultraviolet-ink micropigmentation (invisible tattoos) [39], medical alert bracelets, bootstrapping devices directly communicating with the implanted devices, and active wearable devices (communication cloakers) that act as a third party mediators between the implanted devices and the medical staff [12].

4 Wearable passwords

Passwords and PINs are the dominant mechanism by which we access digital contents. Their key advantages lie in their intangibility: they are readily accessible and can be easily and simply issued, changed, shared or revoked. However, researchers [4, 49, 50] have established that passwords are relatively weak against observation attacks such as shoulder surfing – a potentially serious threat made worse because many users do not perceive it as a significant hazard [20]. Furthermore, passwords lack scalability: while its relatively easy for a user to remember a single password, it is extremely challenging to remember the large set of passwords most modern users possess. This causes many users to write down passwords, further

weakening them against observation. Wearable devices have the potential to address these problems by offering input strategies that are resistant to observation or that prompt or improve the recognition or recall of passwords.

For example, WatchMe [47] is a general purpose ubiquitous input method for smartwatches. It tracks finger movements next to the watch with an embedded camera and displays them as strokes or taps on its screen. The authors envision using the technique for authentication – a number pad is displayed on the watch but the user makes input away from the screen using their finger. The authors argue that the small size of the screen and discrete nature of the finger movements will serve to conceal the entered data from observers.

However, augmented reality glasses such as Google Glass [23, 49], that incorporate fully private personal displays are arguably a more natural fit for authentication via obscured input. Yadav et al. [50] explore the possibilities of this space by comparing authentication via touch or voice on Google Glass. In their system users observe a keypad on the private display showing a random mapping of input symbols to digits. They tap or speak the input symbols to enter the associated PIN items. As attackers are unable to observe the mapping between symbols and digits, no information that can reveal the password is disclosed from the data entry processes. The authors show the technical feasibility of the prototypes and highlight the added security of these methods. Bailey et al. [2] describe a closely related method for voice-input authentication on Google Glass. Instead of a random mapping, users are shown a simple and randomly selected mathematical operation (such as addition of a term) on the private display. They apply this to their PIN items and speak the result. As attackers cannot observe the operation that was applied, listening to the spoken input does not reveal the PIN contents. These examples highlight the potential of using private displays for concealing passwords from bystanders, but showcase the limitations of the input systems on such devices – only voice or low bandwidth forms of touch input are available.

To explore a richer design space, authors have also combined wearable displays with other devices, such as smartphones or external keypads. For example, Winkler et al.'s [49] Glass Unlock presents several methods for combining an unlabeled PIN entry keypad on a smartphone screen with a near-eye display showing the keypad contents. The separation between the input and display device makes observation attacks extremely difficult. Bianchi et al. [4] proposed a conceptually related graphical password system in which users tap pre-selected locations on an image captured from a live video stream. The authors suggest this method would suit wearable computing devices equipped with live video capture capabilities. The video captured by the wearable cameras could be streamed to a mobile device where the user can enter a password by selecting points of interest on the screen [3].

One-Time-Password (OTP) systems can also leverage the cameras in eyeglasses for unlocking wearable devices or establishing a secure connection with external services. Chan et al [7], for example, presented an authentication scheme for unlocking the Google Glass where a QR code displayed on the user's smartphone is scanned using the Glass camera. The credentials contained in the QR code are used to pair the two devices. Khan et al. [27], on the other hand, implemented and evaluated a system that allows a user wearing Glass to scan a QR code containing a OTP to prove co-location to a cloud-based server and obtain a secure PIN template for point-of service authentication.

A final emerging class of wearable authentication system explores the use of thoughts as passwords. Passthoughts [46] presents an early conceptualization of how Brain-Computer Interface (BCI) technology could be used as a password input mechanism. The authors describe the theoretical background and discuss how to "thought-passwords" could be matched reliably against templates. Through a detailed security analysis and consideration of ethical issues they highlight important research challenges for the future of BCI and security. Johnson et al. [26] implemented and evaluated a BCI password by creating a vocabulary of template thoughts and requesting a user select one as a password. This work showcases the potential of using BCI to achieve secure, unobservable passwords.

5 Wearable biometrics

Biometric authentication systems can be classified as explicit, meaning they require a specific dedicated process to measure a bodily characteristic, or implicit, meaning they harvest data about a user in the background and, often, continuously. Wearable systems, with their close proximity to the body, also support hybrid multi-factor approaches that combine explicit and implicit input. The review briefly covers all three classes of system.

Explicit authentication is the most conceptually simple and widely known type of technique. As such, researchers have explored a wide variety of possible channels. For example recent developments in glass-based devices has spurred work on iris recognition [30]. The basic idea is that users would glance into a head mounted camera in order to authenticate. Although iris recognition

systems have been commercialized in other contexts (such as the UK's shelved IRIS border control system), the technology still faces many practical challenges for wearables; research has focused on addressing these. For example, Lee et al. [30] present a method to compensate for distortions from the radial lenses used in head-mounted cameras, improving accuracy and reliability. In order to address imitation attacks, Wang et al. [48] present an algorithm that checks pupil size consistency in varying light conditions. The goal is to protect against image based spoofing of iris recognition processes.

Touch and movement based input have also been proposed as channels for explicit authentication in wearables. Chauhan et al. [8], for instance, successfully classified among a set of users based on gestures performed on the built-in touchpad on the side of Google Glass. Yang et al.'s [51] MotionAuth collects movement data from a wrist-worn device during gesture performance and uses this to verify user identity. The system was tested with a wide range of gestures and was capable of determining whether they were issued by the legitimate user or an imposter with high level of accuracy (2.6% error rate). Roshandel et al. [36] describe Pingu, a broadly similar system that uses motion sensors embedded in a finger ring to identify users as they draw their signatures in the air. The authors demonstrated that features can be extracted and classified with a high level of accuracy: 100% with the 24 users in their sample.

Motion sensors have also been frequently used to achieve implicit authentication. The typical strategy is to continuously read sensor data and use qualities of the recorded movements to identify users. The viability of sensors mounted on a wide variety of body parts in order to capture different movements signals has been investigated. These include: arm mounted sensors to capture swing [16]; ankle mounted sensors to detect foot movements [14]; and lower leg [15], hip [17] or head [31] mounted sensors to assess gait. There is little consensus on optimal mounting points or analysis techniques: user recognition rates in the literature cited above is based on a variety of test scenarios and ranges from 68% to 98%. In an alternative sensing paradigm, body mounted cameras [40, 41] have also been used to perform implicit authentication by inferring gait patterns from video streams. Researchers report this is an accurate approach: 5.6% Equal Error Rate (EER) with a participant pool of 39 users [40].

However, as the properties used for authentication in these systems are gross movements, they are directly observable and may therefore be prone to impersonation attacks. Research suggests this is a legitimate concern. For example, Gafurov et al. [18] demonstrates that an attacker with knowledge about the gait of a set of authentic users can increase their chances of spoofing the system. This suggests that, although simple and unobtrusive, techniques that rely on observable bodily movements open new avenues for attack that may, ultimately, impact the level of security they are able to provide.

Reflecting this problem, researchers have also considered how unobservable body properties, such as electrical profiles, can be used for implicit authentication. Bioamp [24], for example, is a watch-format prototype that senses the impedance of the user's wrist and encodes this as a signal transmitted through the user's body. This data can be sensed by the capacitive touch screen on computer or mobile device and used to disambiguate the user responsible for each touch. While similar technology has been previously proposed [9, 38], Bioamp's authentication application scenario is compelling. The authors highlight use cases for continuous authentication such as personalizing applications to users in real time and displaying confidential data only when users with appropriate access rights are touching the surface.

In terms of hybrid techniques, a common approach has been to combine mature explicit technologies to initially establish user identity (e.g. when a device is put on) followed by implicit approaches that monitor whether or not the device is removed. For example, Ojala et al. [33], describe a hybrid system in a wristband. Initial authentication is achieved via explicit fingerprint entry and recognition that ensures the owner is wearing the device. The wristband then continuously monitors a set of vital signs (skin temperature, heart rate, skin capacitance and motion) and derives a set of implicit measures that it uses to ensure that the device is still worn by the owner. In this way, hybrid approaches combine the strength and conceptual simplicity of explicit methods with the unobtrusive and continuous use enabled by implicit methods.

6 Research opportunities

Although the authentication methods discussed in this review are diverse, there are also clear trends that illustrate promising future avenues for research. We elaborate on four. The first is that authentication interfaces are transitioning from a reliance on physical tokens or passwords to a new focus on automatic collection and recognition of biometric data. Implicit biometrics systems are, as demonstrated in prominent recent work [15, 24, 31], an upcoming research topic that we believe will appear in more and more real-world interfaces over the next decade. Although

this trend is particularly prominent with the wearable devices, it is also evident in the mobile application space [11]. In these systems, the sensors on a smartphone or other portable device collect real time data about context or device use and and infer the identity of the individual carrying or operating them. Due to this widespread applicability, we expect that authentication systems that leverage implicit biometrics will be a rapidly developing research area over the next decade.

The second trend concerns the way authentication systems are conceived by their developers and users. While some wearable authentication work [2, 8, 50] focused on how to authenticate *on* specific devices, more recent work is focusing on authenticating *with* wearable devices. Examples of this new paradigm include systems that enable authentication to public terminals using Google Glass [7, 27, 49] or authenticating to online websites on mobile devices using contents on (or via input on) smartwatches [6]. Although this kind of multi-factor authentication system is an established research topic, the combination of wearable technologies with mobile platforms provides new possibilities because of the computational power and interactive capabilities of the wearables. Rather than serving as simple tokens or transmitters, smart wearables can take a much more sophisticated and diverse role in multifactor authentication schemes. We identify this as an emerging topic with strong potential to yield new forms of authentication technique that provide their users with secure, usable systems.

A third trend concerns the maturity and richness of the technology and tools available in current wearable products. While topics such as implicit authentication and biometrics have long been studied in labs, lack of commercial sensing platforms has restricted the impact of this work on real products and services. With current wearables, this is no longer true as devices typically feature a range of advanced sensors and associated software support such as dedicated Application Programmers Interfaces (API) that provide access to the information they gather. This means that product designers and software developers, as well as researchers, can experiment and implement authentication techniques leveraging these capabilities. Reflecting this reality, we anticipate that novel wearable authentication schemes will reach market more rapidly than with prior technological platforms such as mobiles.

A final issue relates to privacy and wearable devices. The benefits of many of the wearable authentication techniques described in this article exact a toll on privacy. Contextual, biometric or behavioral data is captured, logged, stored or transmitted. In some systems, such as those based on worn cameras, information not only about users, but about those around them may also be recorded. As the backlash against the outward facing camera on the Google Glass indicates [25, 45], users are highly concerned about the privacy implications of wearable sensing and recording technologies. We predict that research exploring the privacy issues and tradeoffs inherent in technologies such as smart tokens capable of tracking workers, or of wireless communicating implantable medical devices will be required before such technologies can enter the mainstream. The scope of this work will be broad, including not only technical but also social and legislative issues. We suggest that methods for preserving privacy when using wearable devices will form a long-term research objective in the security community.

7 Conclusion

Wearable technologies constitute a rapidly developing set of product categories [5, 23] and a dynamic and evolving research field. From the security research perspective, wearable devices provide an opportunity to reenvision and adapt traditional authentication schemes to the new contexts and novel input techniques of wearable devices. The key challenge will be to leverage the strengths and mobility of wearables while bypassing their limitations. In order to contribute to this effort, this paper reviews work on wearable authentication according to the traditional classification of token, passwords and biometric methods. We provided representative examples of authentication interfaces with a variety of wearable form factors such as glasses, wrist watches and rings, as well as highlighting hybrid methods that leverage either multiple devices or multi-factor schemes. The discussion isolates key themes from this literature. It argues that implicit biometric schemes and decentralized authentication systems are relatively unexplored areas that promise strong potential for future research and development. Finally, we also highlighted the inescapable fact that always-on, always-with-us wearable devices raise new privacy concerns for their users. Research that explores how to achieve high security while maintaining privacy will be imperative to the success of future wearable systems.

Acknowledgement: Andrea Bianchi was supported by the MSIP, Korea, under the G-ITRC support program (IITP-2016-R6812-16-0001) supervised by the IITP. Ian Oakley was supported by the 2015 Research Fund (1.150128.01) of UNIST (Ulsan National Institute of Science & Technology).

References

1. J. Al-Muhtadi, D. Mickunas, and R. Campbell. *Wearable security services*. Distributed Computing Systems Workshop, 2001 International Conference on, vol., no., pp. 266–271, 2001.
2. D.V. Bailey, M. Durmuth, and C. Paar. *'Typing' passwords with voice recognition: How to authenticate to Google Glass*. Web: https://cups.cs.cmu.edu/soups/2014/workshops/papers/voice_bailey_20.pdf.
3. A. Bianchi, I. Oakley, and H. Kim. *Using graphical passwords based on optical feature extraction from a live-stream video with wearable or portable devices*. In Korean HCI'14, pp. 641–643, 2014.
4. A. Bianchi, I. Oakley, and H. Kim. *PassBYOP: Bring your own picture for securing graphical passwords*. IEEE Transactions on Human-Machine Systems, pp. 1–10, 2015.
5. Business Insider. *Wearable devices create a new market*, http://www.businessinsider.com/wearable-devices-create-a-new-market-2013-8. Published August 2013. Accessed June 2015.
6. B.R. Cha, S.H. Lee, S.B. Park, G.K. Lee, and Y.K. Ji. *Design of micro-payment to strengthen security by 2 factor authentication with mobile & wearable devices*. Advanced Science and Technology Letters Vol. 109 (Security, Reliability and Safety 2015), pp. 28–32, 2015.
7. P. Chan, T. Halevi, and N. Memon. *Glass OTP: Secure and convenient user authentication on Google Glass*. In Financial Cryptography and Data Security, 8976, pp. 298–308, 2015.
8. J. Chauhan, H.J. Asghar, M.A. Kaafar, and A. Mahanti. *Gesture-based continuous authentication for wearable devices: the Google Glass case*. arXiv preprint arXiv:1412.2855, 2014.
9. C. Cornelius, R. Peterson, J. Skinner, R. Halter, and D. Kotz. *A wearable system that knows who wears it*. In Proceedings of MobiSys '14, pp. 55–67, 2014.
10. M.D. Corner and B.D. Noble. *Zero-interaction authentication*. In Proceedings of MobiCom '02, 1–11, 2002.
11. A. De Luca, A. Hang, F. Brudy, C. Lindner, and H. Hussmann. *Touch me once and i know it's you!: Implicit authentication based on touch screen patterns*. In Proceedings of CHI '12, pp. 987–996, 2012.
12. T. Denning, A. Borning, B. Friedman, B.T. Gill, T. Kohno, and W.H. Maisel. *Patients, pacemakers, and implantable defibrillators: Human values and security for wireless implantable medical devices*. In Proceedings of CHI '10, pp. 917–926, 2010.
13. T. Denning, K. Fu, and T. Kohno. *Absence makes the heart grow fonder: New directions for implantable medical device security*. In Proceedings of USENIX HOTSEC'08, Article 5, 7 pages, 2008.
14. D. Gafurov, P. Bours, and E. Snekkenes. *User authentication based on foot motion*. Signal, Image and Video Processing, 5, p. 457–467, 2011.
15. D. Gafurov, K. Helkala, T. Sondrol. *Biometric gait authentication using accelerometer sensor*. Journal of Computers, 1(7), pp. 51–59, 2006.
16. D. Gafurov, and E. Snekkkenes. *Arm swing as a weak biometric for unobtrusive user authentication*. In Prpceedings of IIHMSP'08 International, pp. 1080–1087, 2008.
17. D. Gafurov, E. Snekkenes, and P. Bour. *Gait authentication and identification using wearable accelerometer sensor*. In IEEE Workshop on Automatic Identification Advanced Technologies, pp. 220–225, 2007.
18. D. Gafurov, E. Snekkenes, and P. Bour. *Spoof attacks on gait authentication system*. In IEEE Transactions on Information Forensics and Security, 2(3), pp. 491–502, 2007.
19. M.T. Goodrich, M. Sirivianos, J. Solis, G. Tsudik, and E. Uzun. *Loud and clear: Human-verifiable authentication based on audio*. Distributed Computing Systems, pp. 10–10, 2006.
20. M. Harbach, E. von Zezschwitz, A. Fichtner, A. De Luca, M. Smith. *It's a hard lock life: A field study of smartphone (un) locking behavior and risk perception*. Symposium On Usable Privacy and Security (SOUPS 2014), pp. 213–230.
21. C. Harrison, M. Sato, and I. Poupyrev. *Capacitive fingerprinting: Exploring user differentiation by sensing electrical properties of the human body*. In Proceedings of UIST '12, pp. 537–544, 2012.
22. H.H. Haung and Y.M. Lin. *Multiple bolts as security devices*. International Symposium on History of Machines and Mechanisms, 355–364, 2009.
23. C. Hill. *Wearables – the future of biometric technology?*. Biometric Technology Today, 2015(8), pp. 5–9, 2015.
24. C. Holz and M. Knaust. *Biometric touch sensing: Seamlessly augmenting each touch with continuous authentication*. In Proceedings of UIST '15, pp. 303–312, 2015.
25. J. Hong. *Considering privacy issues in the context of Google Glass*. Commun. ACM, 56, 11, pp. 10–11, 2013.
26. B. Johnson, T. Maillart, and J. Chuang. *My thoughts are not your thoughts*. In Proceedings of UbiComp '14 Adjunct, pp. 1329–1338, 2014.
27. R. Khan, R. Hasan, and X. Jinfang. *SEPIA: Secure-PIN-authentication-as-a-service for ATM using mobile and wearable devices*. IEEE Mobile Cloud Computing, Services, and Engineering (MobileCloud), pp. 41–50, 2015.
28. S. Kurkovsky, E. Syta, and B. Casano. *Continuous RFID-enabled authentication: Privacy implications*. IEEE Technology and Society Magazine, 30(3), pp. 34–41, 2011.
29. G. Laput, C. Yang, R. Xiao, A. Sample, and C. Harrison. *EM-sense: Touch recognition of uninstrumented, electrical and electromechanical objects*. In Proceedings of UIST '15, pp. 157–166, 2015.
30. J.J. Lee, S. Noh, K.R. Park, J. Kim. *Iris recognition in wearable computer*. Biometric Authentication, 3072, pp. 475–483, 2004.
31. S. Li, A. Ashok, Y. Zhang, C. Xu, J. Lindqvist, and M. Gruteser. *Whose move is it anyway? Authenticating smart wearable devices using unique head movement patterns*. To appear in PerCom'16.
32. N. Matsushita, S. Tajima, Y. Ayatsuka, and J. Rekimoto. *Wearable key: Device for personalizing nearby environment*. International Symposium on Wearable Computers, pp. 119–126, 2000.
33. S. Ojala, J. Keinanen, and J. Skytta. *Wearable authentication device for transparent login in nomadic applications environment*. Signals, Circuits and Systems, pp. 1–6, 2008.
34. B. Phillips. *The Complete Book of Locks and Locksmithing (Sixth Edition)*. McGraw-Hill, 2005.
35. E.R. Post, M. Reynolds, M. Gray, J. Paradiso, and N. Gershenfeld. *Intrabody buses for data and power*. International Symposium on Wearable Computers, pp. 52–55, 1997.
36. M. Roshandel, A. Munjal, P. Moghadam, S. Tajik, and H. Ketabdar. *Multi-sensor finger ring for authentication based on 3D*

signatures. In Human-Computer Interaction. Advanced Interaction Modalities and Techniques, 8511, pp. 131–138, 2014.
37. V. Roth, P. Schmidt, and B. Guldenring. *The IR ring: Authenticating users' touches on a multi-touch display*. In Proceedings of UIST '10, pp. 259–262, 2010.
38. M. Sato, I. Poupyrev, and C. Harrison. *TouchÃ©: Enhancing touch interaction on humans, screens, liquids, and everyday objects*. In Proceedings of the CHI '12, p. 483–492, 2012.
39. S. Schechter. *Security that is meant to be skin deep: Using ultraviolet micropigmentation to store emergency-access keys for implantable medical devices*. In Proceedings of USENIX HealthSec 2010, pp. 1–2, 2010.
40. K. Shiraga, N.T. Trung, I. Mitsugami, Y. Mukaigawa, and Y. Yagi. *Gait-based person authentication by wearable cameras*. In Networked Sensing Systems (INSS), pp. 1–7, 2012.
41. Y. Shen, C. Luo, W. Xu, and W. Hu. *Poster: An online approach for gait recognition on smart glasses*. In Proceedings of SenSys '15, pp. 389–390, 2015.
42. F. Stajano. *Security Issues in Ubiquitous Computing*, Handbook of Ambient Intelligence and Smart Environments, pp. 281–314, 2010.
43. K. Suhonen, K. Vaananen-Vainio-Mattila, and K. Makela. *User experiences and expectations of vibrotactile, thermal and squeeze feedback in interpersonal communication*. In Proceedings of BCS-HCI '12, pp. 205–214, 2012.
44. D.Z. Sun, J.P. Huai, J.Z. Sun, J.W. Zhang, and Z.Y. Feng. *A new design of wearable token system for mobile device security*. IEEE Transactions on Consumer Electronics, 54(4), 1784–1789, 2008.
45. The Atlantic. *WHow the camera doomed Google Glass*, http://www.theatlantic.com/technology/archive/2015/01/how-the-camera-doomed-google-glass/384570. Published January 2015. Accessed June 2015.
46. J. Thorpe, P.C. van Oorschot, and A. Somayaji. *Pass-thoughts: Authenticating with our minds*. Web: https://eprint.iacr.org/2005/121.pdf.
47. W. Van Vlaenderen, J. Brulmans, J. Vermeulen, and J. Schoning. *WatchMe: A novel input method combining a smartwatch and bimanual interaction*. In Proceedings of CHI EA '15, pp. 2091–2095, 2015.
48. T. Wang, Z. Song, J. Ma, Y. Xiong, and Y. Jie. *An anti-fake iris authentication mechanism for smart glasses*. Communications and Networks (CECNet), pp. 84–87, 2013.
49. C. Winkler, J. Gugenheimer, A. De Luca, G. Haas, P. Speidel, D. Dobbelstein, and E. Rukzio. *Glass unlock: Enhancing security of smartphone unlocking through leveraging a private near-eye display*. In Proceedings of CHI '15, pp. 1407–1410, 2015.
50. D.K. Yadav, B. Ionascu, S.V.K. Ongole, A. Roy, and N. Memon. *Design and analysis of shoulder surfing resistant PIN based authentication mechanisms on Google Glass*. In Financial Cryptography and Data Security, 8976, pp. 281–297, 2015.
51. J. Yang, Y. Li, and M. Xie. *MotionAuth: Motion-based authentication for wrist worn smart devices*. In PerCom Workshops'15, pp. 550–555, 2015.

Bionotes

Andrea Bianchi
KAIST, Department of Industrial Design,
Daejeon, Republic of Korea
andrea@kaist.ac.kr

Andrea Bianchi received the B.S. degree in business from Universita Commerciale Luigi Bocconi, Milano, Italy, in 2004, the M.S. degree in computer science from New York University, New York, NY, USA, in 2007, and the Ph.D. degree in culture technology from the Korea Advanced Institute of Science and Technology (KAIST), Daejeon, Korea, in 2012. He is currently an Assistant Professor with the Department of Industrial Design, KAIST. His research focuses on human-computer interaction, wearables and tangible interaction.

Ian Oakley
Department of Human and System Engineering, UNIST,
Ulsan, Republic of Korea
ian.r.oakley@gmail.com

Ian Oakley received the joint B.S. degree (Hons.) from the Schools of Computing Science and Psychology, University of Glasgow, Glasgow, U.K., in 1998, and the Ph.D. degree from the School of Computing Science, University of Glasgow, in 2003. He is currently an Associate Professor with the Department of Human and System Engineering, Ulsan National Institute of Science and Technology, Ulsan, Korea. His current research interests include human-computer interaction and, specifically, multimodal, physical, tangible, and social computing.