Outsmarting Proctors with Smartwatches: A Case Study on Wearable Computing Security

Alex Migicovsky, Zakir Durumeric, Jeff Ringenberg, and J. Alex Halderman

University of Michigan, Ann Arbor MI 48109, USA
{amigi,zakir,jringenb,jhalderm}@umich.edu

Abstract. Many companies have recently started to offer wearable computing devices including glasses, bracelets, and watches. While this technology enables exciting new applications, it also poses new security and privacy concerns. In this work, we explore these implications and analyze the impact of one of the first networked wearable devices—smartwatches—on an academic environment. As a proof of concept, we develop an application for the Pebble smartwatch called ConTest that would allow dishonest students to inconspicuously collaborate on multiple-choice exams in real time, using a cloud-based service, a smartphone, and a client application on a smartwatch. We discuss the broader implications of this technology, suggest hardware and software approaches that can be used to prevent such attacks, and pose questions for future research.

Keywords: security, wearable computing, smartwatches, cheating

1 Introduction

Recent hardware advances have led to the development and consumerization of wearable computing devices ranging from exercise and sleep tracking bracelets [6] to augmented reality glasses [8]. While these new technologies enable a spectrum of new applications, they also introduce security and privacy questions that are largely unexplored.

The introduction of smartphones created important new risks to users' privacy due to their mobility, ubiquity, and wealth of sensors—wearable computing form factors are likely to magnify these threats. For instance, while smartphone malware can hijack the sensors to spy on the user, video-capable smartglasses or smartwatches are worn continuously outside the clothing where they are even better positioned to record both the user's activities and those of others nearby.

Beyond risks to the user's own privacy, wearables have the potential to be maliciously deployed by the users themselves to violate the security and privacy of others. These threats will be particularly acute in coming years: as wearables gradually become widespread and inconspicuous, they will challenge longstanding social norms and violate expectations about the capabilities of technology. For instance, glasses and wristwatches are socially acceptable in situations where

[*] Revised January 31, 2014. For the latest version, visit https://jhalderm.com/papers/.

the use of smartphones and computers might not be and they can be used to surreptitiously capture and exfiltrate data in violation of privacy expectations.

In this paper, we examine a second dimension in which wearables challenge existing threat models: they have the potential to secretly receive data or perform computations in ways that confer an underhanded advantage to the user, such as helping count cards in a casino or cheating on an exam. Although wearables encompass a diverse range of form factors, we focus on smartwatches because they are among the first feature-rich and programmable wearable devices to reach a broad consumer audience.

As a proof of concept, we examine how smartwatches can lead to realistic attacks on an academic testing environment. Using the Pebble smartwatch platform, we demonstrate a prototype cloud-backed application called ConTest that would enable dishonest students to covertly collaborate on multiple-choice exams. We also discuss defensive countermeasures for this class of attacks and use the perspective of this case study to draw broader security lessons about the future of wearable computing technologies.

2 Related Work

Most prior work has focused on the security of wearable devices themselves and on the privacy of the data produced by these technologies [9,12,13,14,18]. However, there has been little work exploring the implications of such devices within current day society, despite increasing interest [20]. In this work, we primarily focus on the implications of new wearable devices and how users can potentially abuse these devices—not on securing the devices themselves or the data they produce.

Another interesting aspect of our example attack is that it relies on multiple devices with different feature sets to execute the attack. A smartwatch alone may not pose security risks, but combining features of many wearables may allow for security vulnerabilities. This concept was investigated by Denning et al. as it applied to household robots [4].

There has also been previous work on the dynamics of cheating outside of the computational space [3,7,10]. However, a large portion of the research assumes that users may only collaboratively cheat if test takers are sitting side-by-side [10]. The attack we introduce eliminates this restriction.

There is growing precedent for students using emerging technology to cheat. In one widely reported case, a student in Thailand was caught using a watch with phone capabilities to send text messages during an exam [21]. In another instance, a man taking a driver's license test used a small video camera to send live video of the questions to a remote party who helped him correctly answer them via an earpiece [15]. Students have also used programmable graphing calculators, Bluetooth pens, and invisible ink to cheat on exams [17]. Such high-tech cheating may become even more widespread as wearable devices gain in popularity and decrease in detectability.

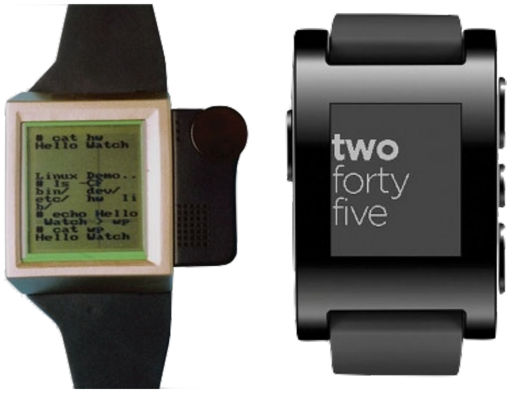

Fig. 1: *Left*: IBM created this Linux smartwatch prototype in 2000, but it was never commercialized; image adapted from [16]. *Right*: The Pebble Smartwatch came on the market in 2012.

3 Smartwatches

Wristwatches have evolved significantly over the last half-century from the introduction of the first digital watches in the 1960s to what we now term "smartwatches"—fully programmable watches with the capability to interact with other devices and Internet services [11]. The first smartwatch was introduced in 2000 by IBM, which demonstrated a prototype watch running Linux and powered by an ARM processor (Figure 1; *left*). The device was bulky and the prototype was never commercialized [16].

In late 2012, Pebble Technology released the first successful consumer smartwatch (Figure 1; *right*) after receiving funding through Kickstarter. As of July 2013, more than 85,000 of the devices had been sold [2]. The most recent version of the watch includes an ARM Cortex-M3 processor, a 144 × 168 pixel black-and-white e-paper display, Bluetooth 4.0, a vibrating motor, digital compass, accelerometer, and Lithium-ion battery. Pebble provides a software development kit (SDK) that allows programmers to create applications for the watch and provides APIs for Bluetooth communication, local storage, time synchronization, graphics drawing, and button and vibration control.

Today's smartwatches have relatively limited hardware capabilities compared to smartphones or laptops, limiting the set of security mechanisms that can be applied locally within the devices. Furthermore, the Pebble architecture places a large amount of trust in the user's smartphone, with which the watch pairs via Bluetooth. An app on the phone is responsible for updating the watch's firmware, transferring data to and from the Internet, and installing and managing apps on the watch, all of which compounds the watch's attack surface. However, advances in technology are likely to remove these limitations in future generations of smartwatches and other wearable devices.

4 ConTest: Cheating by Smartwatch

In order to illustrate some of the disruptive security implications of wearable technologies such as smartwatches, we developed ConTest, an application for the

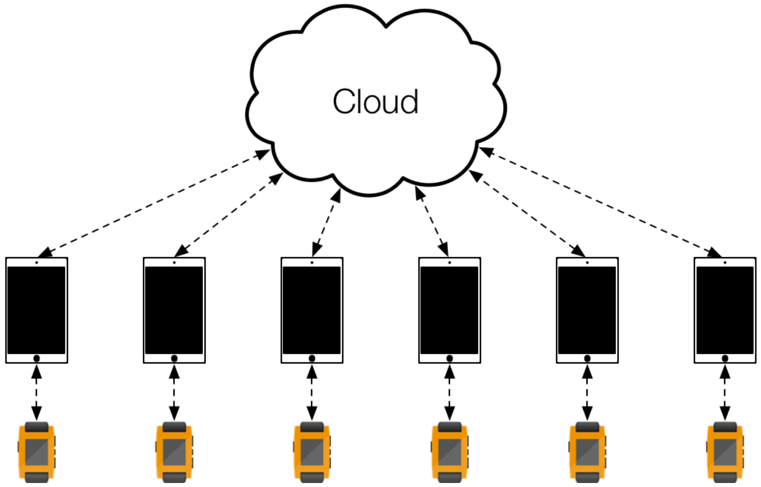

Fig. 2: **ConTest Architecture** — A light-weight app on the Pebble smartwatch interfaces via Bluetooth with a control app running on a smartphone. The smartphone app in turn communicates with a centralized cloud-based service.

Pebble smartwatch that is designed to allow dishonest students to inconspicuously share and vote on answers during multiple-choice exams in real-time. Society's expectations about the capabilities of wristwatches have yet to catch up to the new capabilities of devices such as Pebble. While smartphones are prohibited in many exams, including the ACT and SAT, digital watches are currently allowed [1,19]. ConTest is nearly indistinguishable from a standard watch, provides a difficult-to-notice user interface, and allows students to cheat in a manner similar to if they had readily available access to a smartphone during an exam.

ConTest is composed of three components: a client application for the Pebble smartwatch that allows users to vote and view the collaboratively decided solutions, a cloud-based service that coordinates answer sharing, and an application for the smartphone that relays data between the smartwatch and the central service. The application architecture is shown in Figure 2.

Cheating by smartwatch presents a realistic threat today. Pebble smartwatches are available for $150, smartphones have become ubiquitous among students, and web hosting providers such as Amazon EC2 and Heroku are available for free or at negligible cost. Even if used among a small conspiracy of students, ConTest has potential for impacting exam scores, because research has shown that a dishonest student needs to view the collective answers of only four students in order to perform satisfactorily on an exam [10].

Cloud Application A cloud-based server provides a central service that stores and aggregates exam responses submitted by individual users. It determines the most common response to each question and distributes it back to each smartwatch as necessary. This central service could also potentially perform more

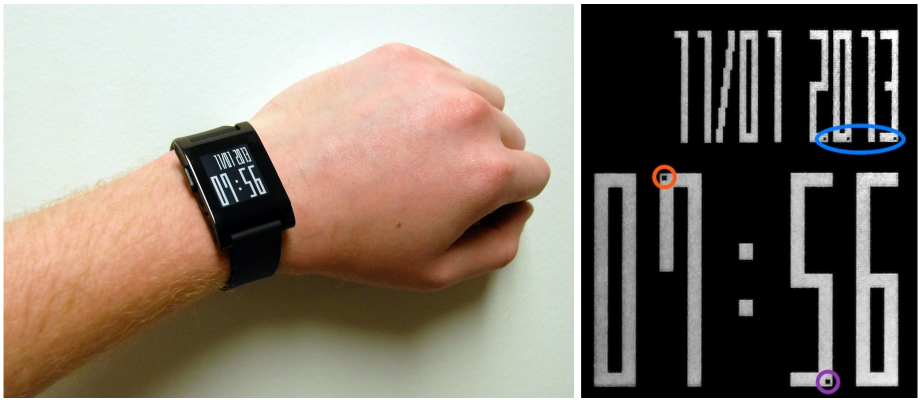

Fig. 3: **ConTest Prototype** — At a distance (*left*), the application appears to be an innocuous clock face. Closer inspection reveals the question number and answer displays (*right*), encoded in groups of missing pixels.

complex calculations, such as distinguishing between multiple forms of an exam or allowing a third-party to authoritatively provide answers instead of relying on crowdsourced solutions. We implemented the server using Ruby on Rails and hosted it via Heroku.

Smartphone Application Before entering a testing environment, a student pairs a Pebble smartwatch with a smartphone and installs a smartphone app that allows them to select the exam they are going to take. During the exam, the smartphone app relays data between the Pebble and the cloud-based server. While the attack does require a smartphone for communication, no further interaction is required on the smartphone during the exam itself. The smartphone can remain out of sight in the student's jacket or backpack. The smartphone app runs on iOS and is implemented using the iOS and Pebble SDKs.

Smartwatch Application The smartwatch component of ConTest allows users to both provide and view collaboratively decided answers. In order to make the app more difficult for proctors or other test takers to notice, the correct date and time are shown on the watch face as usual. The questions and answers are indicated by inverting small groups of noncritical pixels, as shown in Figure 3.

The answer to the selected question is encoded by mapping each of the digits in the time to an answer and inverting a small number of pixels in the digit to indicate its selection. For example, in Figure 3, the purple-circled block of missing pixels in the five indicates that the user has voted for answer D and the red-circled block of pixels in the seven indicates that the most popular answer selected by other users is B. As seen in the figure, this surreptitious form of displaying answers is clear to the user at close range, but practically invisible to anyone examining the watch from a longer distance.

The user can vote for a particular answer by double-clicking the watch buttons. When a user changes their vote, the new answer is immediately relayed to the

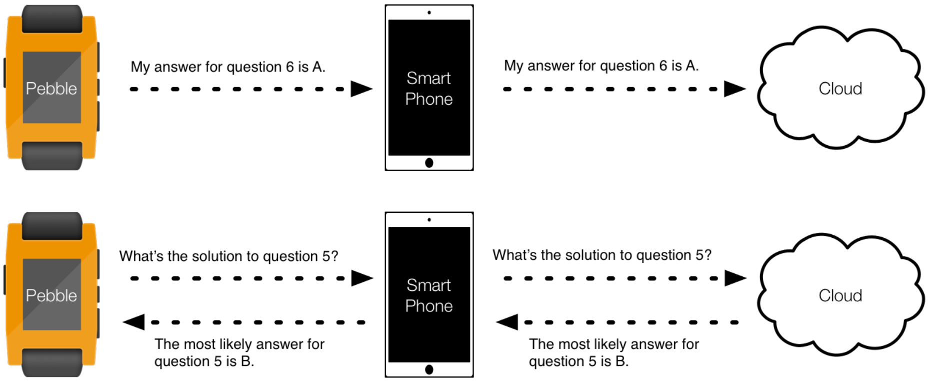
Pebble
My answer for question 6 is A.
Smart Phone
My answer for question 6 is A.
Cloud
Pebble
What's the solution to question 5?
The most likely answer for question 5 is B.
Smart Phone
What's the solution to question 5?
The most likely answer for question 5 is B.
Cloud

Fig. 4: **ConTest Protocol Schematic** — When providing answers (*top*), the smartwatch app transmits test answers volunteered by users to the cloud-based service. When receiving answers (*bottom*), the app queries the service for the answer to a numbered question and receives the consensus response.

service and other watches. A similar approach is used to choose the question number. The selected question number is encoded in binary in the date. For example, the blue-circled digits in Figure 3 indicate that the displayed solution is for question 13. The selected answer can be changed by single-clicking the built-in buttons on the watch.

5 Defenses and Lessons

The obvious solution for preventing students from cheating using smartwatches is to ban the devices from exams. Even as smartwatches become commonplace and harder to distinguish, it would not be out of the question to ban all types of wristwatches and to instead provide wall clocks. The Graduate Record Examination (GRE) has adopted a policy along these lines in which it bans all forms of digital watches from its examination centers [5]. Exams can also be constructed to be more resilient to such attacks, particularly if the test is computerized, by randomly selecting and ordering questions and answers.

However, while it may be be obvious to ban smart devices in controlled environments such as during an exam or at a casino, this may not be feasible in other situations such as at public events. Devices will continue to evolve, both decreasing in size and detectability and improving in terms of processing power, sensing capability, and connectivity. As wearable devices begin to include features such as integrated cameras and direct Internet connectivity, there is further potential for abuse such as covertly monitoring private meetings. Further, as these technologies continue to become integrated into our daily lives, e.g. smartglasses that are integrated with prescription eye-ware, users may be dependent on these wearables, making it burdensome for users to simply remove a device.

While wearables are likely have disruptive security effects, the computing and communication capabilities of these devices might also be harnessed to create new countermeasures. One simplistic approach would be to implement software-based restrictions that could be switched on by an external signal or when the device recognizes it is in a special environment, such as an exam mode that disables third-party applications on the Pebble. However, such restrictions might be readily bypassed if the devices are not locked down by the manufacturer. Future work is needed to determine whether wearable devices can be designed with flexible, safe, and guaranteeable restrictions.

6 Conclusion

Wearable technologies offer an exciting platform for new types of applications and have the potential to more tightly integrate computing within daily life. However, they also pose new security and privacy concerns. Wearables are prone to many of the same attacks as smartphones, but they may pose increased risks due to their novel form factors. Many questions arise over the privacy of the data collected by these devices, and their potential to inconspicuously record and stream sensor data in social settings. In this work, we explored another new security dimension, how wearable devices can be maliciously used by their owners to violate existing security paradigms.

We introduced ConTest, an application for the Pebble smartwatch that can be used by dishonest students to collaboratively cheat on multiple-choice exams. ConTest demonstrates that today's wearable technology already poses a meaningful threat to existing threat models, and future wearable devices are likely to be even more disruptive. Although preventing cheating by banning such devices from testing environments may be somewhat effective, in the long run, threat models will need to be revised to take into account the rapidly increasing capabilities of wearable computing.

Acknowledgements

The authors wish to thank Martin Strauss for insightful guidance and Phil and Jill Migicovsky for early help and feedback. This work was supported in part by the National Science Foundation (NSF) under contract numbers CNS 1111699 and CNS 1255153.

References

1. ACT, Inc. What should I take to the test center?, 2013. http://www.actstudent.org/faq/bring.html.
2. Arthur, C. Dell eyes wearable computing move as PC business keeps slumping. The Guardian, 2013. http://www.theguardian.com/technology/2013/jul/04/dell-wearable-computing-pc-business.

3. Cizek, G. J. *Cheating on Tests: How to Do It, Detect It, and Prevent It.* Routledge, 1999.
4. Denning, T., Matuszek, C., Koscher, K., Smith, J. R., and Kohno, T. A Spotlight on Security and Privacy Risks with Future Household Robots: Attacks and Lessons. In *Proceedings of the 11th International Conference on Ubiquitous Computing* (2009), Ubicomp '09, pp. 105–114.
5. Educational Testing Service. On test day, 2013. http://www.ets.org/gre/revised_general/test_day?WT.ac=grehome_gretestday_130807.
6. Fitbit, Inc. Fitbit Force, 2013. http://www.fitbit.com/.
7. Frary, R. B., Tideman, T. N., and Watts, T. M. Indices of cheating on multiple-choice tests. *Journal of Educational and Behavioral Statistics 2*, 4 (1977), 235–256.
8. Google. Google Glass, 2013. http://www.google.com/glass/start/what-it-does/.
9. Halderman, J. A., Waters, B., and Felten, E. W. Privacy management for portable recording devices. In *Proceedings of the Workshop on Privacy in the Electronic Society* (2004), pp. 16–24.
10. Harpp, D. N., and Hogan, J. J. Crime in the classroom: Detection and prevention of cheating on multiple-choice exams. *Journal of Chemical Education 70*, 4 (1993).
11. Hochet, B., Acosta, A., and Bellido, M. *Integrated Circuit Design. Power and Timing Modeling, Optimization and Simulation: 12th International Workshop (PATMOS).* Springer, 2002.
12. Hong, J. I., and Landay, J. A. An architecture for privacy-sensitive ubiquitous computing. In *Proceedings of the 2nd International Conference on Mobile Systems, Applications, and Services* (2004), ACM, pp. 177–189.
13. Kagal, L., Finin, T., and Joshi, A. Trust-Based Security in Pervasive Computing Environments. *Computer 34*, 12 (2001).
14. Langheinrich, M. Privacy by design—principles of privacy-aware ubiquitous systems. In *Ubicomp 2001: Ubiquitous Computing* (2001), Springer, pp. 273–291.
15. McWhirter, C. High-tech cheaters pose test. The Wall Street Journal, 2013. http://online.wsj.com/news/articles/SB10001424127887324069104578529480125489370.
16. Narayanaswami, C., Kamijoh, N., Raghunath, M., Inoue, T., Cipolla, T., Sanford, J., Schlig, E., Venkiteswaran, S., Guniguntala, D., and Kulkarni, V. IBM's Linux watch, the challenge of miniaturization. *Computer 35*, 1 (2002), 33–41.
17. Osborne, C. How do students use tech to cheat?, 2012. http://www.zdnet.com/blog/igeneration/how-do-students-use-tech-to-cheat/14216.
18. Saponas, T. S., Lester, J., Hartung, C., Agarwal, S., Kohno, T., et al. Devices That Tell on You: Privacy Trends in Consumer Ubiquitous Computing. In *Usenix Security* (2007), vol. 3, p. 3.
19. The College Board. SAT test day checklist, 2013. http://sat.collegeboard.org/register/sat-test-day-checklist.
20. Wagner, D., et al. Security and Privacy for Wearable Computing. Panel discussion, 2008. https://www.usenix.org/conference/hotsec13/security-and-privacy-wearable-computing.
21. Wong-Anan, N. Watch out! Thai exam cheat triggers phone-watch ban. Reuters, 2008. http://www.reuters.com/article/2008/03/05/us-thailand-cheating-idUSBKK4207420080305.