English

T.I.M.

Contrôle 1

October 2018

Note pour les surveillants:

- Durée 1h30
- **Aucun document et pas de dictionnaire.**
- Brouillon recommandé

- **Ne rendre que la feuille réponse**

Why wearables are computing's future

By Alistair Fairweather

1. For many technophiles, 2013 was a slightly disappointing year. Sure, there were one or two **groundbreaking** launches (such as Google Glass), but for the most part it was a year of consolidation rather than raw innovation. This year is likely to be more exciting as several waves of long-awaited technology finally begin to peak.

Wearable computing

2. What is the most **ubiquitous** technology on the planet? No, it's not the television or even the car—it's the cellphone. The International Telecommunication Union has predicted that during 2014 the global cellphone market will pass 100% penetration. In other words, there will be more active cellphone subscribers (both prepaid and post-paid) on the planet than there are people.

3. Now, imagine that you could wear your phone like a watch or a pair of spectacles. Instead of having to dig around in your pocket or bag to answer a call or look up something on the Internet, you could simply speak a command and the device would obey.

4. That, in a nutshell, is the promise of wearables: instantly accessible computing integrated into both your wardrobe and your daily life.

5. Two major wearable computing devices were launched in 2013: Google Glass (which looks like a pair of spectacles) and Samsung's Galaxy Gear (a "smart watch"). Both are more prototypes than mature products. Negative reviews have flooded in — they are "expensive", "buggy", "bulky" and their battery life is "appalling". Blogs with titles such as White Men Wearing Google Glass have been launched, dedicated to ridiculing anyone caught using them in public.

6. Had blogs existed in the late 1980s, there would have been several dedicated to scoffing at pretentious cellphone owners. The earliest cellphones were expensive, **ludicrously** bulky, did not work particularly well and had terrible battery life. They were little more than status symbols for the technologically obsessed. And yet, by the mid-1990s, the cellphone market was booming.

7. Although wearable computing will not reach mainstream acceptance for at least another five years, 2014 will see a **slew** of new devices entering the market, both from established players such as Apple (the long-awaited iWatch) and from relatively new entrants such as FitBit (which focuses on the activity tracking market).

8. The volume of ridicule will also grow as more nerdy trailblazers take the **plunge** into wearables. But I predict that within 10 years the wearable computing market will be as big as the smartphone market is today, and within 20 it will be bigger than the entire global cellphone market.

NSA-proof communication

9. The second half of 2013 was dominated by revelations of indiscriminate and unjustifiable snooping by America's National Security Agency (NSA) and the British Government Communications Headquarters. Leaks by Edward Snowden, a former NSA contractor, have revealed an appalling disregard for the privacy of innocent civilians and allies alike.

10. One of the most shocking revelations was the mechanism through which NSA operatives are able to compel large service providers such as Google and Facebook to release private data to them. Secret courts issue secret federal warrants for this data, and the companies are forbidden to warn the targets or disclose the contents of these warrants.

11. These **blatant** attacks on privacy have fuelled demand for communication platforms and standards that both organisations would be unable to penetrate. Riseup, a service that allows political dissidents in repressive countries to communicate securely with one another, is being overwhelmed by demand for new accounts. Its founders have launched a fundraising drive to expand its capacity.

12. Because Riseup refrains from storing any information that might allow anyone to identify its users, even if the NSA did seize its servers it would find little of any use. Riseup also encrypts all of the data it stores. Without the keys to that encryption, even the combined computing might of both organisations would take millennia to unscramble the data.

13. Particularly cautious Riseup users can connect to the service with a virtual private network. This technology **conceals** their location from anyone who may be tapping the network by routing all traffic through an intermediate server. Anyone tracing the connection will only be able to find the location of that intermediate server, not the user.

14. Another initiative, Darkmail, is developing a new standard aimed at making e-mail immune to surveillance. The idea is to send encrypted e-mails directly between trusted users — a method known as "peer to peer" — rather than through centralised servers, which is where messages are most often intercepted. Its founders hope Darkmail will become so popular with smaller service providers that the likes of Microsoft and Google will be forced to adopt it.

15. Both of these are nonprofit initiatives, but several commercial service providers will jump on the bandwagon before the end of 2014. For ordinary people with nothing to hide, the pain of abandoning their trusty Gmail or Yahoo addresses will be too much to bear, but the paranoid will **flock** to these new islands of privacy.

Smart televisions

16. For the better part of 20 years, the promise of smart TV has been like cold fusion: great in theory but impossible in practice. Every attempt was dogged by intractable problems such as incompatibility of standards, awful user interfaces, **lack** of sufficient content and slow Internet connectivity.

17. And so, though our phones and our computers have become smarter and smarter, our TVs have remained as dumb as they were in the 1980s. But in the past three years a perfect storm has been forming that will, in 2014, make the smart TV a mainstream reality.

18. Devices such as Google's Chromecast, Apple TV and Boxee have solved the compatibility and user interface problems at a stroke. You simply plug them into one of the standard ports on your TV set and, voilà, you have a smart TV.

19. Content used to be controlled entirely by the broadcasters. Now services such as Netflix, iTunes and Hulu offer catalogues so vast that even the most esoteric and discerning tastes are **catered** for (and usually at a fraction of the price charged by the broadcasters).

20. Internet connectivity is improving around the globe, if somewhat unevenly. Although South Africa remains one of the worst laggards in terms of broadband roll-out and affordability, an average middle-class family can afford an uncapped broadband connection without having to sell any children into slavery.

21. Today, anyone with a **modicum** of technical skill (or a geeky friend) can access legal, on-demand Internet content on their television set. At the moment, South African bandwidth prices make this option slightly more expensive than local pay-TV services, but those prices will tend to fall over time. And so, increasingly, people will begin cancelling their DStv subscription in favour of services such as Netflix and Hulu.

22. Because of its effective monopoly over sports coverage, MultiChoice will be protected from this phenomenon of "cord cutting" for at least another five years. But on-demand Internet TV is too powerful a force to resist for long. The likes of Google and Apple do not care about the MultiChoices of the world — they will simply go around them.

23. Of course, television manufacturers are not taking this invasion of their **turf** lying down. Scarred by years of unprofitability and bogged down by outdated thinking, most TV makers have struggled to get the formula right. Some, such as Samsung and LG, are beginning to make headway but they have a long way to go. Still, most people's first experience of smart TV will probably be through one of these "native" platforms.

All answers should be written on the given answer sheet.

The next two exercises are based upon the **"Why wearables are computing's future"** article.

Part 1. Key words: Fill the gaps below using one of the key words **in bold** from the text.

1. A ____X____ of something is a reasonable but not large amount of it.
2. If there is a ____X____ of something, there is not enough of it.
3. If you describe something as ____X____, you are emphasizing that you think it is foolish, unreasonable, or unsuitable.
4. A ____X____ war is a struggle between people over who controls a particular activity.
5. If you go into an activity or are ____X____ into it, you suddenly get very involved in it.
6. You use ____X____ to describe something bad that is done in an open or very obvious way.
7. If people ____X____ to a particular place or event, a very large number of them go there.
8. A ____X____ of things is a large number of them.
9. If you describe something or someone as ____X____, you mean that they seem to be everywhere.
10. You use ____X____ to describe things which you think are significant because they provide new and positive ideas.

Part 2. Find the word: find the following words in the text.

1. An adjective that means that it is simple, powerful, and real. (between para 1 – 3)
2. An expression that means that you are searching in a place or container. (between para 1 – 3)
3. An adjective that implies that something is large and heavy but also difficult to deal with. (between para 5 – 7)
4. An adjective that means that something is so bad or unpleasant that it shocks. (between para 5 – 7)
5. A verb that describe a state of mind when feelings or events affect you very strongly, and you do not know how to deal with them. (between para 9 – 11)
6. A verb that implies that you are deliberately not doing something. (between para 12 – 14)
7. When people, activities or ideas are described with this adjective, they are regarded as the most typical, normal, and conventional. (between para 16 – 17)
8. An adjective that means that something is not under any kind of restriction whatsoever. (between para 19 – 21)
9. An adjective that means that something prevents you from making progress or getting something done. (between para 22 – 23)
10. A verb that implies that you are trying hard to do something, also when people or things may be making it difficult for you to succeed. (between para 22 – 23)

All answers should be written on the given answer sheet.

Two Dudes Prove How Easy It Is to Hack ATMs for Free Cash.

(An ATM is also called a cash distributor.)

By Kevin Poulsen

1. When a small-time Tennessee restaurateur named Khaled Abdel Fattah was running short of cash he went to an ATM. Actually, according to federal prosecutors, he went to a lot of them. Over 18 months, he visited a slew of small kiosk ATMs around Nashville and withdrew a total of more than $400,000 in 20-dollar bills. The only problem: It wasn't his money.

2. Now Fattah and an associate named Chris Folad are facing 30 counts of computer fraud and conspiracy, after a Secret Service investigation uncovered evidence that the men had essentially robbed the cash machines using nothing more than the keypad. Using a special button sequence and some insider knowledge, they allegedly reconfigured the ATMs to believe they were dispensing one dollar bills, instead of the twenties actually loaded into the cash trays, according to a federal indictment issued in the case late last month. A withdrawal of $20 thus caused the machine to spit out $400 in cash, for a profit of a $380.

3. The first $20 came out of one of their own bank accounts. That's right: They were using their own ATM cards.

4. "They were little kiosk ATMs, like you would find in a business or a convenience store," says Greg Mays, assistant special agent in charge of the US Secret Service's Nashville office. "I believe the businesses noticed there was a problem when the machine was running out of money."

5. As charged, the plan is an unusually successful example of a low-tech ATM hack that's been used for minor theft in the past, and a reminder of the security weaknesses that have troubled kiosk ATMs. Vulnerabilities in the most popular machines made by Tranax Technologies and Trident were showcased in a now-legendary "ATM jackpotting" demonstration delivered by security researcher Barnaby Jack at the Black Hat conference in 2010. Jack (who died last year) showed that the Tranax machines could be hacked into and reprogrammed remotely over dial-up, and the Trident ATMs could be physically opened and then reprogrammed through a USB port. The companies responded to Jacks' research by closing those holes.

6. But at the street level, criminals have exploited a simpler vulnerability that requires no hacking software or gear: Unlike the machines deployed at bank locations, kiosk ATMs could be placed into a privileged "operator mode" simply by pressing a special sequence of buttons on the ATM keypad.

7. From that mode, you could manipulate a number of variables—one of which sets the denomination of the bills loaded into the machine's currency cartridges.

8. A supposedly secret six-digit numeric password protects the Operator Mode, but in the Nashville case, one of the defendants, Fattah, was a former employee of the company that operated the machines, says the Secret Service's Mays, so he knew the code.

9. Fattah allegedly recruited his friend Folad into the scheme, and in January 2009 they began visiting the cash machines. First they'd use the code to change the denomination register on the machine, then they'd make their withdrawals, and finally change the configuration back.

Repeating the scam all over town, by March 2010 they'd pulled down $400,000 between them—money the government is now hoping to seize.

10. Contacted by WIRED, Folad referred inquiries to his attorney. "Unfortunately, I am not in a position to discuss anything at the moment," Folad said in an e-mail. His lawyer also declined to comment. Fattah, who now owns a well-reviewed restaurant in Nashville, didn't return phone calls about the October 22 indictment.

11. The government says the men made a few mistakes in the thefts, including being captured on surveillance video while making withdrawals, and, of course, using debit cards issued under their real names.

12. The amount of money taken in Nashville—$400,000—is unusually high, but plenty of other thieves have pulled the same currency-switching scam with more modest returns, and without Fattah's inside knowledge. Most don't make the mistake of using their own debit cards, opting instead to buy a prepaid debit card, the kind anyone can pick up at a Walgreens.

13. Around 2005, criminals discovered that the default factory-set master passcodes for the Tranax and Trident ATMs were printed right in the service manuals, which were readily available online. Triton's master passcode was "123456."

14. The manuals suggested machine owners immediately change the passcodes from the defaults, but many of the small business owners who favor the inexpensive, pedestal-sized machines never made the change. That led to an uncommon phenomenon in the world of cyber-crime: hacking as a street crime. After spreading quietly for at least 18 months, the scheme went viral in 2006 when a man was caught on a surveillance tape looting an ATM at a Virginia gas station. CNN ran the video, and the truth of the default passcodes surfaced.

15. Both Tranax and Triton promptly tweaked the programming for new ATMs to force operators to change the default passcodes on first use. Machines already deployed, though, were still vulnerable, and reports of more incidents followed. In 2007, a Derry, Pennsylvania, convenience store called Mastrorocco's Market was hit for $1,540 by an unidentified man in flip flops and shorts. In 2008, two 21-year-old men hit Lobo's City Mex in Lincoln, Nebraska, for $1,400 in three separate visits–on the fourth, the son of the store owner pulled a gun on them and called the police. In 2010, a North Carolina grocery worker plotted to hit 30 different ATMs while wearing a wig, but his plan was thwarted when an associate turned him in to the FBI. He was sentenced to 37 months.

16. Currency switching schemes appear to be rare now, says David Tente, executive director of the ATM Industry Association, though hard data is difficult to come by. "Nobody likes talking about fraud, especially when it's against them," Tente says. "Independent operators and financial institutions are very tight lipped about this sort of thing."

17. But there's some evidence that operator passcodes are still an issue, he notes. Last June, two 14-year-old boys in Winnipeg followed internet instructions to gain operator access to a Bank of Montreal ATM at a grocery store, successfully guessing the six digit master passcode. The boys immediately notified the bank, which changed the code.

18. Who knows how many ATM hackers have been less scrupulous?

All answers should be written on the given answer sheet.

The next two exercises are based upon the **"Two Dudes Prove How Easy It Is to Hack ATMs for Free Cash"** article.

Part 3. Find the word or phrase in the article that is a synonym for the following.

1. A word that means claimed, but not yet proven (para 2)
2. A verb meaning to confiscate (para 9)
3. A verb meaning to choose (para 12)
4. An adjective that means unmodified (para 13)
5. A verb that means to prevent smothing from happening (para 15).

Part 4. Indicate whether the following statements about ATM thefts are "**true**", "**false**" or "**not given**" in the article.

1. In order to prevent future cases of ATM fraud, companies are holding conferences to educate their customers.
2. Despite steps to fix the situation, operator access is still easy to get on some machines.
3. The two robbers mentioned in the article could never have gotten caught if they avoided using machines with cameras.
4. Hacking an ATM does not require special computer skills.
5. Companies have been aware of the problem but only took steps to correct it after the general public found out.

Part 5. Match the following names to the action in the article they are most responsible for (They can be used more than once.) Write the full name and first name onto your answer sheet

Barnaby Jack	Chris Folad	David Tente	Khaled Abdel Fattah	No one

1. Reported on people who have raised awareness of how easy it was to re-program ATM's.
2. Believes statistics on ATM fraud would be easier to get if businesses were more willing to talk openly about it.
3. Revealed security weaknesses at an event.
4. Will spend the next 18 months in prison for 30 counts of computer fraud and conspiracy.
5. Spent 18 months traveling all around the US stealing money.

All answers should be written on the given answer sheet.