SWITCHcert Security Report

October 2014

I. Same again? Fingerprint sensor on new iPhone 6 hacked using same method as for previous model

Apple has plenty to celebrate. It claims that more than 10 million people bought a new iPhone 6 over the first weekend after it went on sale – a new record. However, it is likely to be less delighted by the news that the new fingerprint sensor – which heise.de points out is not new at all – has already been hacked using the exact same method as the Chaos Computer Club, among others, used to trick the previous model's «Touch ID».

Lookout blogger Marc Rogers has also cracked Touch ID, but he comes to an ambivalent conclusion in his post on the subject: «Touch ID is great for locking the iPhone, and it will keep most people out, but when it comes to really sensitive data, you should consider another security measure.» There are several reasons for this. Touch ID locks your iPhone 6 after five failed attempts. A higher resolution and larger scanning area are also intended to ensure that creating a usable spoof or false fingerprint requires considerably more skill, patience and precision. However, Touch ID, with its easily fooled sensor, also opens up access to third-party apps such as the password safe 1Password as well as to contactless payments via the NFC-based Apple Pay. This could mean that a hacked iPhone 6 has much more serious consequences for its rightful owner than was the case with the prior model.

While Apple claims that Touch ID is both very convenient and highly secure, the fundamental question of whether biometric security features make sense given the risks they entail remains, regardless of any specific security concerns relating to individual functions. See also our Security Report article on this topic from September 2013, in which Hamburg-based data protection expert Johannes Casper was quoted as saying that biometric data cannot be deleted and should thus never be left behind unless it is absolutely necessary. This warning is every bit as valid now as it was then.

Read more here:

http://www.inside-it.ch/articles/37692

http://www.heise.de/security/meldung/Fingerabdrucksensor-des-iPhone-6-ueberlistet-2399891.html

http://www.ccc.de/en/updates/2013/ccc-breaks-apple-touchid

https://blog.lookout.com/blog/2014/09/23/iphone-6-touchid-hack

http://arstechnica.com/security/2014/09/fake-fingerprint-fools-iphone-6-touch-id-why-its-not-so-serious

http://www.switch.ch/export/sites/default/all/cert/downloads/secrep/_files_secrep/Sec-Report_September_2013.pdf

II. Up in the air: drones, balloons and unresolved security issues

The analysts of US aerospace research firm Teal Group claim that sales of military and civilian drones will grow to more than USD 89 billion (approx. CHF 86 billion) a year within ten years. A significant share of this will be accounted for, in the most literal sense, by Amazon, DHL and other logistics operators. Added to these are the Internet service providers intending to put hitherto unconnected regions of the world online using drones (Facebook) or balloons (Google). Also contributing to the increase in air traffic alongside the military will be intelligence services, police forces, journalists, film-makers, photographers and hobbyists.

Civilian unmanned aerial vehicles (UAVs) and remotely piloted aircraft (RPAs) are already being used to transport supplies and conduct search-and-rescue missions in hard-to-reach places such as Haiti and Bhutan. DHL recently began testing parcel deliveries to the North Sea island of Juist, 12 km from the mainland. Facebook, meanwhile, will test drones in 2015 aimed at bringing Internet access to deprived areas.

Google's Project «Loon» is even further advanced. According to the company, it will provide an entire country with permanent Internet access in 2015 using balloons floating 20 km above the ground. The spectrum of unmanned aircraft goes from simple quadrocopters flown for fun to the Global Hawk, which is used by civilian organisations and can fly for 40 hours non-stop with a range of 20,000 km.

The technology is evolving at an astonishing pace, but a number of questions remain unanswered. These concern protection against spying, public safety, the security of data collected and transmitted by drones and privacy. NASA is working with the start-up Airware to develop an automated air traffic control system that will monitor and manage drone traffic in four to five years' time. Most civilian UAVs, however, are relatively simple to hack and hijack, and reports of drone crashes are increasingly common. The latest example is the as yet unexplained crash of one of the Zurich police's CHF 30,000 drones on 3 October.

Read more here:

http://www.tagesanzeiger.ch/zuerich/stadt/Drohne-der-Polizei-ist-abgestuerzt/story/25181885

http://www.zeit.de/digital/internet/2014-09/drohnen-hacken-gps-star-wars

http://www.tagesschau.de/wirtschaft/post-drohne-alltag-101.html

http://resources.infosecinstitute.com/privacy-security-issues-usage-civil-drones

http://futurezone.at/digital-life/nasa-entwickelt-flugverkehr-kontrollsystem-fuer-drohnen/85.522.462

http://futurezone.at/digital-life/facebook-startet-bald-internet-drohnen-tests/87.507.428

https://www.steigerlegal.ch/2014/07/10/drohnen-schweiz-verschaerft-regeln-per-1-august-2014

http://www.heise.de/tr/artikel/Google-Projekt-Internet-per-Ballon-auf-der-ganzen-Welt-2403375.html

III. Google's Transparency Report shows Swiss authorities becoming more data-hungry

Compared with the almost 32,000 requests to hand over user data that Google received in the second half of 2013 according to its latest Transparency Report, 124 requests from Swiss authorities appears to be an insignificant number. However, it is highly significant in that it represents an increase of more than 50% relative to the prior period, which is well above the global average growth rate. Google's Transparency Report states that government authorities around the world submitted 15% more information requests as part of police investigations, with rises of 19% in the US and 44% in Germany.

Richard Salgado, Director for information security and law enforcement matters, stresses that Google endeavours to provide information only where all the applicable legal requirements are met. Even so, data had to be given out in roughly half of all cases.

Read more here:

http://www.computerworld.ch/marktanalysen/studien-analysen/artikel/schweizer-behoerden-wollen-immer-mehr-von-google-wissen-66425/

http://www.forbes.com/sites/emmawoollacott/2014/09/16/google-piles-pressure-on-congress-with-latest-transparency-report/

http://www.handelsblatt.com/technologie/it-tk/it-internet/anfragen-bei-google-und-facebook-deutsche-behoerden-sind-besonders-neugierig/9772564.html

http://de.statista.com/infografik/844/auskunftsersuchen-zu-nutzerdaten-von-behoerden-und-gerichten-bei-google/

IV. Hacked through your fridge: how secure is the Internet of Things?

Armbands, cars and refrigerators have little in common on the surface. In the age of wearables, smart homes and connected cars, however, they are all linked via the Internet. Cisco estimates that there will be roughly 50 billion networked devices by 2020. Since everything that is on the network can be hacked, it is worth looking into the issue of security. The results are anything but comforting. David Jacoby of Kaspersky Lab, for instance, noted that, while he had suitably protected all his normal IT, one piece of network hardware had a hidden root access with the single digit "1" as its password and was thus open as wide as a barn door to potential attackers. We must therefore ask ourselves how effectively wearables, smart homes and connected cars are protected against misuse. Plausible threat scenarios are not hard to find.

Wearables: A CEO's Nike FuelBand or Apple Watch, to name just two examples, could be hacked by a rival firm or even «just» a headhunter in order to gain an insight into the manager's health and thus gauge the chances of staging a hostile takeover or determine whether he might be receptive to a job offer more effectively than by talking to him. His own company, meanwhile, could check data from his golf watch to see how much time he spends away from the office.

Smart homes: Nest is a small AI device that records the activities of the people living in a house and uses these data to produce and store programmes for controlling the lights, heating etc. Hacking in and reading these would be very a useful aid for burglars or kidnappers. There is only a short step from having a bathroom device such as the Philips Apothecary record its users' health data every single morning to health insurers installing a transmitter in exchange for a discount on premiums that leads to good behaviour being rewarded with lower costs and the promise of increased benefits while bad habits are penalised with higher costs and reduced benefits.

Connected cars: This is already a reality to some extent with car insurers offering «black box» recorders – within the law and with their customers' consent, of course. But what happens when a jealous husband or a cheated wife is able to manipulate a connected car's accelerator pedal, or when a 20-year-old Bash bug can be used on connected cars? «Shellshock» could take on a whole new meaning in this context.

Read more here:

http://www.heise.de/security/meldung/Internet-der-Dinge-Die-Zahnbuerste-als-Gefahr-2400670.html

http://www.golem.de/news/smarthome-die-ifa-wird-zur-messe-der-sicherheitsluecken-1408-108841.html

http://www.golem.de/news/internet-der-dinge-ameisengrosse-radios-sollen-die-welt-verbinden-1409-109174.html

http://www.scip.ch/?labs.20140716

https://nest.com/thermostat/life-with-nest-thermostat

http://www.design.philips.com/about/design/designportfolio/design_futures/design_probes/projects/microbial_home/apothecary.page

http://www.bankinfosecurity.com/interviews/shellshock-bug-how-to-respond-i-2463

The Clipboard: Interesting Presentations, Articles and Videos

Criminals are increasingly making use of the new top-level domains such as .support, for example to make phishing mails look as authentic as possible:

http://www.csoonline.com/article/2687132/social-engineering/recently-introduced-tlds-create-new-opportunities-for-criminals.html

Adam Caudill and Brandon Wilson gave a talk on BadUSB at the DerbyCon security conference in Louisville, Kentucky and published their hacks. Caudill told the tech magazine Wired, «People see USB sticks as nothing more than storage devices. They don't realise there's a reprogrammable computer in their hands.»

http://www.irongeek.com/i.php?page=videos/derbycon4/t510-making-badusb-work-for-you-adam-caudill-brandon-wilson

http://www.wired.com/2014/10/code-published-for-unfixable-usb-attack/

Environmentally friendly Bitcoin mining: Ken Shirriff shows how to work out the hash function SHA-256 used in the mining process with a pencil and paper:

http://www.righto.com/2014/09/mining-bitcoin-with-pencil-and-paper.html

http://www.youtube.com/watch?v=y3dqhixzGVo

The SWITCHcert Security Report was written by Dieter Brecheis and Frank Herberg.

It does not reflect the opinions of SWITCH but is instead a summary of articles published in various media. SWITCH accepts no liability for the content or opinions contained in the Security Report or for its correctness.