SWITCHcert Security Report

January 2015

SWITCH

I. iBeacons: the next big thing for 2015?

Apple has introduced a new indoor navigation standard called iBeacon that transmits using Bluetooth Low Energy (BLE). Its range is limited to just 30 metres, but IT and trade experts are expecting it to set off nothing less than a major revolution in terms of personalised real-time communication and data analysis, with the market growing as large as USD 4 billion within the next three years. The new technology allows apps to send a signal to mobile devices running iOS 7/Android 4.3 or higher, for example to notify them of special offers on the shelves and then direct them towards the shortest queue at the till. An iBeacon-enabled app could replace the audio guide in a museum or guide visitors to their seat at a stadium, theatre or concert venue, perhaps even offering them an upgrade on the way. This is already the case at 20 US baseball stadiums. Schools, universities and libraries might use iBeacons to help people find their way around.

Of course, all of this can only work if the system knows the location of the smartphone and thus of its owner. The price of using iBeacon services is disclosing information on where you walk, how long you spend browsing shelves or looking at exhibits, what you buy or view and so on. The scope this provides for tracking and profiling has many data miners rubbing their hands in anticipation. This is why data protection advocates are calling for transparency. At the same time, iBeacons are not unproblematic for the

people operating them. Rivals or reward junkies could clone them: «…it is easy to trick reward systems that rely on you being somewhere. Like 'get a free coffee if you enter our shop 100 times'».

Read more here:

http://startups.co.uk/tech-trends-for-2015-the-ibeacon

http://www.sueddeutsche.de/digital/beacon-technologie-in-kaufhaeusern-rabatt-schlacht-auf-dem-smartphone-1.2047755

http://www.absatzwirtschaft.de/marketingentscheider-setzen-auf-die-nutzung-von-ibeacons-40829

http://www.huffingtonpost.com/rebecca-abrahams/what-ibeacon-may-mean-for_b_4964375.html

http://www.absatzwirtschaft.de/besteht-eine-hinweispflicht-auf-ibeacons-17558

http://airfy.svbtle.com/clone-a-beacon-ibeacon-and-the-proof-of-location-issue

II. «Locate. Track. Manipulate.»: a new level of mobile snooping

The quote at the start of our headline is actually the title of an advertising brochure from the New York-based supplier of the SkyLock mobile tracking software. The *Washington Post* recently published the brochure to demonstrate how global tracking systems, previously thought to be the preserve of tech-savvy organisations like the US National Security Agency or its British counterpart GCHQ, can now be bought by just about anyone on the open market and used to nefarious ends. Commentators fear that this pushes «geoslavery», the term coined by geoinformation system researchers Jerome E. Dobson and Peter F. Fischer to describe the negative impact of geodata tracking, to a whole new level. Tobias Engel explained this and how global mobile tracking via the SS7 signalling protocol works at the recent 31st Chaos Communication Congress (31C3).

In addition to creative use of SS7, there is also talk of devices called IMSI catchers following revelations in the leading Norwegian newspaper *Aftenposten* in December. These imitate mobile base stations and can intercept and manipulate any mobile activity within range. *Aftenposten* discovered six of these fake base stations in central Oslo alone. The *Washington Post* reported back in September that it had found 18 in and around Washington, D.C.

Read more here:

http://www.washingtonpost.com/business/technology/for-sale-systems-that-can-secretly-track-where-cellphone-users-go-around-the-globe/2014/08/24/f0700e8a-f003-11e3-bf76-447a5df6411f_story.html

https://www.msu.edu/~kg/874/geoslavery.pdf

http://www.nzz.ch/international/europa/wie-die-totale-handy-ueberwachung-funktioniert-1.18456550

http://www.aftenposten.no/nyheter/iriks/Secret-surveillance-of-Norways-leaders-detected-7825278.html

http://www.washingtonpost.com/world/national-security/researchers-try-to-pull-back-curtain-on-surveillance-efforts-in-washington/2014/09/17/f8c1f590-3e81-11e4-b03f-de718edeb92f_story.html

III. How to steal fingerprints with a 200-mm zoom lens

Hacker Jan Krissler knows a lot about fingerprints. He researches security procedures at Berlin's Technische Universität and showed as long ago as 2008 how easy it was to identify, copy and misuse a fingerprint unwittingly left behind on a water glass – specifically, a glass that had been used by the then German Interior Minister Wolfgang Schäuble. He has now produced further proof that fingerprints are not exactly an ideal security tool. Using Verifinger, a piece of software costing EUR 400, and a photo of Ursula von der Leyens's right hand taken from three metres away with the kind of 200-mm zoom lens commonly used by press photographers, he succeeded in faking the fingerprint of Mr Schäuble's colleague from the Ministry of Defence. While he was moving in government circles, he thought he might as well take a photo of Chancellor Merkel's iris 110 pixels across and use it to create another biometric fake.

Two months before that, MasterCard and a Norwegian biometrics firm had presented a new type of credit card that replaces the PIN with the card holder's fingerprint. The testing partner, Norway's Sparenbanken DIN, said that the technology is to be employed for all of the payment cards it offers. We do not yet know whether the bank has reconsidered and opted to supply a pair of non-see-through gloves with each card following Krissler's appearance at 31C3...

Read more here:

http://www.zeit.de/digital/datenschutz/2014-12/fingerabdruck-merkel-leyen-hack-ccc-31c3

http://www.nzz.ch/mehr/digital/jan-krissler-starbug-chaos-communication-congress-31c3-fingerabdruck-von-der-leyen-1.18452235

http://www.theregister.co.uk/2014/10/18/mastercard_adds_fingerprint_scanner_to_credit_card_for_pinless_transactions

IV. Drones – buzzing business, more stringent rules and fewer benefits than expected

According to the Consumer Electronics Association (CEA), the drone business is really buzzing. During its Consumer Electronics Show (CES) in Las Vegas in the second week of January, the CEA published market research figures suggesting that consumer drone sales would grow by 55% to USD 130 million in 2015, equating to around 400,000 units. The CEA predicts that drones sales will exceed USD 1 billion over the next five years. However, the proliferation of drones in the air is already causing headaches for some, as evidenced by the near miss between a drone and an Airbus at London's Heathrow Airport last summer. The French authorities identified an entirely different security threat in October: drones flying over several of the country's nuclear power stations.

Switzerland has also introduced new rules for drone flights. The city of Zurich, whose police force lost a CHF 30,000 drone last summer in an unexplained crash (as we reported in October) has completely banned drone flights over public land, while flights over private land require the owner's permission. The federal government allows flights over crowds only with a permit and sets up no-fly zones for major events like the World Economic Forum and last year's Organization for Security and Co-operation in Europe conference in Basel.

The U.S. Inspector General, meanwhile, has criticised the U.S. Customs and Border Protection Agency's drone use for being too expensive and ineffective. Tom Barry, an Analyst at the Center for International Policy, says, «I don't want to say drones have no place in border control, but expensive, military-grade drones have not proven effective in catching immigrants or stopping drug flows.»

Read more here:

http://tech.firstpost.com/news-analysis/ces-2015-the-drone-revolution-begins-with-airdog-hexo-and-nixie-248607.html

http://www.tagesschau.de/ausland/drohnen-ueber-akw-in-frankreich-101.html

http://www.nzz.ch/zuerich/stadt-zuerich/drohnen-verbot-ueber-zuerich-1.18439947

http://www.steigerlegal.ch/2014/12/01/osze-drohnen-flugverbot-und-helikopter-bordschuetzen

http://yaleglobal.yale.edu/content/drone-patrols-us-border-ineffective-report-finds

V. The Golden Globes in the wake of the Sony hack

«Tonight we celebrate all the movies North Korea was OK with.» This was how hosts Tina Fey and Amy Poehler alluded to the hack of the Sony Pictures and PlayStation Network servers at the Golden Globes on 11 January, adding a cultural perspective to the technical, criminal and political facets of the story. Since the hack was made public on 24 November, it has been covered so intensively in the media and sparked so much speculation over the perpetrators and their motives that the best thing for us to do here is provide links to an updated history and Bruce Schneier's comments. The third link is recommended for some not entirely serious punditry – every time you refresh, a new combination of hacker and motive appears.

Read more here:

https://www.riskbasedsecurity.com/2014/12/a-breakdown-and-analysis-of-the-december-2014-sony-hack
https://www.schneier.com/blog/archives/2014/12/did_north_korea.html
http://sony.attributed.to

The Clipboard: Interesting Presentations, Articles and Videos

The talks from the recent Chaos Communication Congress, including those on fingerprint photography and the SS7 hack, are available online:

http://media.ccc.de/browse/congress/2014/

Who's Attacking Whom? Brian Krebs has put together some splendid dynamic visualisations of Internet attacks:

http://krebsonsecurity.com/2015/01/whos-attacking-whom-realtime-attack-trackers/

The people at howtogeek.com investigated what happens when you download the top 10 apps on, say, download.com:

http://www.howtogeek.com/198622/heres-what-happens-when-you-install-the-top-10-download.com-apps/

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