SWITCHcert Security Report

August 2016

SWITCH

I. Sheer tracking pleasure – debate on information sovereignty and transparency in relation to vehicle data shifts up a gear

Connected cars, the data they collect and the question of who these data actually belong to and who can do what with them is a topic we have touched on a number of times in the Security Report. Now the German automobile club ADAC has investigated exactly what data are logged by a BMW i3, a BMW 320d, a Mercedes B-Class and a Renault ZOE. In terms of privacy, the results are quite sobering. All four models collect far more data than mechanics really need for on-board diagnostics. The Mercedes, for instance, transmits not only its GPS position, mileage, fuel consumption and tyre pressure to the manufacturer every two minutes, but also the number of times the seatbelts tighten. This can be used to draw conclusions about driving behaviour. Similar data can be extracted from both of the BMWs. The Renault, meanwhile, is an open book as far as data are concerned. Renault can use a mobile connection and the ZOE's Controller Area Network (CAN) bus to read virtually any piece of information on the car that takes its interest. On top of this, if the lease payments for the battery are not made in time or in full, Renault can override the charging process at any time and thus immobilise the car.

BMW, for its part, has paradoxically stated that it does not store location data from customers' cars, only to go ahead and supply the regional court in Cologne with

precisely this kind of data, making it possible to trace the exact movements of a DriveNow customer. DriveNow, a car-sharing joint venture between BMW and Sixt, claimed that it only records the time and place of the pick-up and drop-off. However, the Cologne court said that the data it received were from BMW itself. BMW admitted that the car has several systems logging data but insisted that these could not be used to trace the driver's movements (which would be at best problematic and at worst illegal under current German data protection law). BMW actually refused to comment any further on the grounds of data protection!

The police in North Rhine-Westphalia seem less than impressed with BMW's «sheer tracking pleasure» as well. According to their press spokesman, they had a clause added to the lease agreement for their new BMW patrol cars requiring the manufacturer to make its network provider deactivate the embedded SIM cards.

The Automotive Warranty & Recall Report 2016 contains details of a very different problem concerning connected and software-driven cars. It has evidence that increasingly complex IT controls are making cars massively more susceptible to faults and vastly increasing the recall rate. This, despite the fact that, in the words of security expert David Kenny, the supposedly high-tech interfaces most of today's cars use are based on low-tech standards from the 1980s and in some cases even the 1970s and were «never designed with security in mind».

Read more here:

http://www.heise.de/newsticker/meldung/ADAC-Untersuchung-Autohersteller-sammeln-Daten-in-grossem-Stil-3227102.html
https://www.adac.de/infotestrat/technik-und-zubehoer/fahrerassistenzsysteme/daten_im_auto/default.aspx?ComponentId=260789&SourcePageId=8749&quer=daten
http://www.tagesschau.de/wirtschaft/adac-ueberwachung-auto-101.html
http://www.zeit.de/mobilitaet/2016-02/datenschutz-autos-adac-aufklaerung-transparenz
http://www.manager-magazin.de/unternehmen/autoindustrie/bmw-autobauer-liefert-gericht-kundendaten-fuer-bewegungsprofil-a-1104050.html
https://netzpolitik.org/2016/bmw-speichert-keine-standortdaten-gibt-aber-bewegungsprofil-an-gericht
https://netzpolitik.org/2016/neue-streifenwagen-in-nrw-uebermitteln-keine-daten-an-bmw
http://www.computerworld.ch/news/security/artikel/automobile-immer-mehr-rueckrufe-wegen-software-problemen-70306
http://www.techinsider.io/hacker-car-hacking-2016-6

II. Improving security on the Internet of Things – latest news from the Guardian Project and Riffle, a joint venture between MIT and EPFL

When previously standalone devices (including cars, as outlined above) are suddenly networked, data security is often no more than an afterthought – if it is thought about at all. We discussed this in the Security Report back in September 2014, and there has been little or no progress since then. The issue is now being addressed by the Guardian Project, a global collective of people from a variety of professions that has set itself the goal of providing open-source software and security apps. One of these is Home Assistant, a new open-source platform for controlling all of the networked devices in a building. Home Assistant is innovative in that it can be configured to use the anonymous Tor network to connect devices to the Internet. This makes it much harder to hack into them and track their use. The project is designed as a proof-of-concept study, so it is not yet ready for the marketplace, but founder Nathan Freitas says, «Our goal is to show this can work and hopefully advocate towards commercial product vendors.» The security measures put in place by these product vendors often amount to no more than equipping networked devices with a security code and setting it to 0000 by default.

The Guardian Project is not to be confused with comic-book legend Stan Lee's superheroes-meet-National Hockey League collaboration of the same name, which was much more commercial in its ambitions. Also unconnected with Freitas's project is Teddy the Guardian. The cute teddy bear and other cuddly Guardian toys feature an array of sensors that tell parents about their children's health via an app.

More news on anonymous networks comes from Cambridge, Massachusetts and Lausanne. Researchers from the Massachusetts Institute of Technology (MIT) and the Federal Institute of Technology Lausanne (EPFL) are working on an alternative to Tor that provides something Tor cannot, namely formal proof of security. The system, called Riffle, works with a mixnet. Messages from different sources are encrypted and mixed together before they are sent. Every server that forwards the mix package has to prove that it has not made any changes. Riffle's developers argue that, while this makes it less efficient than Tor, it also makes it much more secure. They stress that they are not trying to replace Tor but rather to offer an alternative, and they also point out that Riffle is still in development.

Read more here:

http://www.theverge.com/circuitbreaker/2016/7/22/12251714/tor-smart-hub-iot-security-guardian-project
https://theintercept.com/2016/07/20/tor-could-protect-your-smart-fridge-from-spies-and-hackers
https://blog.torproject.org/blog/quick-simple-guide-tor-and-internet-things-so-far
https://www.youtube.com/watch?v=m8CkvrCiikE
http://www.nhl.com/ice/page.htm?id=66928
http://teddytheguardian.com
http://futurezone.at/produkte/stofftiere-sammeln-daten-ueber-die-gesundheit-von-kindern/209.192.015
http://www.spiegel.de/netzwelt/web/riffle-neue-tor-alternative-soll-noch-mehr-sicherheit-bieten-a-1103766.html
https://techcrunch.com/2016/07/11/mits-anonymous-online-communications-protocol-riffle-could-beat-tor-at-its-own-game
http://www.ictjournal.ch/News/2016/07/13/Le-MIT-et-lEPFL-imaginent-un-reseau-danonymisation-plus-fort-que-Tor.aspx

III. Summer 2013 revisited – could SFG/FURTIM make the nightmare scenario of a blackout reality?

In 2013, we recommended Marc Elsberg's novel «Blackout» as a thrilling summer read that gives some food for thought regarding aspects of security. It seemed that the book's fictional scenario might become real when researchers from endpoint security specialists SentinelOne reported a supervisory control and data acquisition (SCADA) attack on a European energy group. The malware dubbed SFG, they said, was effectively the «parent» of the FURTIM strain and attacks control systems used in industrial automation. Security firm Dalballa, on the other hand, postulated that SFG and FURTIM are closely related but not focused on specific applications. SentinelOne then published a clarification stating emphatically that its analysis of the malware had been misinterpreted and that SFG/FURTIM was no laughing matter. The malware, it said, is so sophisticated that it attacks at three levels and also evades antivirus software and firewalls that use static and heuristic techniques. To avoid detection, it can identify systems with biometric access control and sandbox environments and encrypt itself when pursued. Based on its complexity and refinement, the researchers suspect that it is state-sponsored. Numerous clues point towards an Eastern European country.

The question of how well – or indeed how badly – critical infrastructure is protected against unauthorised access or even manipulation thus remains as contentious as ever. Both Golem.de and internetwache.org claim to have gained access to control systems at water works, power and heating plants, building automation systems and other industrial control systems around the world within the space of a few weeks.

Read more here:

https://securityblog.switch.ch/2013/07/31/sommerlekture-blackout
http://www.finanzen.net/nachricht/aktien/SentinelOne-entdeckt-staatlichen-SCADA-Angriff-auf-westeuropaeischen-Energiekonzern-4981504
http://www.theregister.co.uk/2016/07/18/firm_calls_bullshit_on_scada_malware
https://sentinelone.com/blogs/sfg-furtims-parent
http://www.golem.de/news/schwachstellen-aufgedeckt-der-leichtfertige-umgang-mit-kritischen-infrastrukturen-1607-122063.html
http://derstandard.at/2000041246620/Oesterreichische-und-deutsche-Kraftwerke-und-Smart-Homes-ueber-Internet-angreifbar

IV. Cruel summer 2016 – cybercriminals jumping on the Pokémon GO bandwagon

Google currently delivers some 77 million hits for this summer's biggest fad. Launched on 6 July 2016, Pokémon GO is the augmented reality version of Nintendo's console blockbuster from 20 years ago, which has since given rise to an entire entertainment ecosystem – including no fewer than 18 feature films. With over 200 million games sold, the Pokémon universe is one of the most lucrative product ideas in the history of gaming. It therefore comes as no surprise that some want to jump on the bandwagon and exploit its success for their own ends. As ever, there are plenty of unscrupulous freeloaders using faked apps and even a supposedly «official» Pokémon GO Facebook page to lure players into handing over money and/or data. As well as explaining how to play the game, Giga.de has posted explicit warnings about phishing attempts, subscription traps and other kinds of cyber fraud. Some old-school criminals are also using the game's augmented reality element as a means of attracting victims to a particular place via the virtual realm and then robbing them in a very real way.

Read more here:

http://futurezone.at/games/pokemon-go-betrug-mit-gewinnspielen-und-fake-apps/210.702.019
http://www.giga.de/spiele/pok-mon-go/specials/pokemon-go-gewinnspiel-fake-vorsicht-vor-phishing-und-abofallen
http://www.theverge.com/2016/7/10/12142434/pokemon-go-armed-robberies-missouri

V. Not everyone is chasing Pokémon – Google Sheep View and the Faroe Islands

A whole year before Pokémon GO conquered our streets, Ding Ren and Michael Karabinos from the Netherlands used the fact that 2015 was Year of the Sheep as the inspiration for their photo project Google Sheep View. Instead of cartoon monsters, they collect images of sheep they find on Google Street View. They explain that the project has no affiliation with Google.

Daruta Dahl, meanwhile, does want to work directly with Google on her commission for the Faroe Islands Tourist Board. Because the far-flung islands are not represented on Google Street View, she has started a project entitled SheepView 360, equipping five sheeps with 360-degree cameras, a mobile phone and solar panels and sending them out to roam the fields. The aim is to portray the islands in a media-friendly way and inform tourists about the best spots to visit. You can see just how green the grass is on the Faroe Islands from the comfort of your own home at http://visitfaroeislands.com/sheepview360.

Read more here:

http://www.googlesheepview.com/about
https://www.theguardian.com/travel/2016/jul/12/sheep-view-360-faroe-islands-google-mapping-project
http://www.faz.net/aktuell/gesellschaft/tiere/google-sheep-view-auf-den-faroeern-14339363.html
http://futurezone.at/digital-life/sheepview360-kamera-schafe-scannen-faeroeer-inseln-ein/209.583.637

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