# SWITCHcert Security Report

March 2016


SWITCH

## I. Torpedoed for a fistful of dollars – university helps authorities spy on Tor users

In his day, Andrew Carnegie was the richest man in the US. He put some of the fortune he made in the steel industry into building the Carnegie Technical Schools to provide vocational training for the sons and daughters of his workers in Pittsburgh. Little did he know that, just a century later, they would have become one of the most expensive universities in the western world: Carnegie Mellon University (CMU). Such luminaries as Andreas von Bechtolsheim (co-founder of Sun Microsystems), Charles Geschke (co-founder of Adobe) and James Gosling (inventor of Java) studied at CMU's renowned School of Computer Science. With this in mind, it should be clear how shocked the IT community was to hear that CMU's Software Engineering Institute (SEI) had accepted a payment of at least USD 1 million from the FBI for its help in deanonymising Tor users with a view to identifying and apprehending people dealing drugs on the Silk Road 2.0 trading platform. This accusation was made by the Tor Project itself in a blog post on 11 November. A spokesman for the university immediately denied it and challenged the Tor Project to produce hard evidence to back up its claims, stressing that he had no knowledge of any payment from the FBI.

The trial of a man named Brian Farrell has now shed rather more light on the topic. According to the prosecution, Farrell used the Tor network to deal drugs on the illegal online marketplace Silk Road and was identified through deanonymisation. At the request of Farrell's defence team, details of how the FBI tracked him down have now been disclosed: the SEI did indeed conduct research for the purpose of deanonymising Tor users. It remains unclear how the research project came to the FBI's attention. What is clear, however, is that it was not the FBI that commissioned and paid for the project but the Department of Defense. Both the university and the Pentagon are maintaining a steely silence on the matter, appropriately enough given CMU's origins.

The people in charge of the Tor Project were dismayed and disappointed at the judge's response to their claim that the research work undermined the privacy of all Tor users. Judge Richard Jones argued that Tor users willingly share their public IP address with the first Tor node and can thus have no reasonable expectation of privacy while using the network. The Tor people countered that Jones had failed to understand the whole concept of anonymous surfing on the Tor network and made it clear that they had already closed the privacy gaps torn open by the SEI researchers.

Read more here:

https://blog.torproject.org/blog/did-fbi-pay-university-attack-tor-users
https://www.wired.de/collection/latest/die-carnegie-mellon-university-hat-angeblich-fuer-geld-das-tor-netz-gehackt
http://motherboard.vice.com/read/carnegie-mellon-university-attacked-tor-was-subpoenaed-by-feds
http://www.golem.de/news/silk-road-verfahren-tor-nutzer-koennen-keine-privatsphaere-erwarten-1602-119388.html
https://de.wikipedia.org/wiki/Carnegie_Mellon_University
http://www.zeit.de/digital/datenschutz/2016-02/darknet-pentagon-bezahlt-forscher-angriff-auf-tor
https://blog.torproject.org/blog/statement-tor-project-re-courts-february-23-order-us-v-farrell

## II. Crypto Wars 3.0 – will the FBI be given a licence to snoop, or can Apple successfully lock down the unlocking?

Legal and ethics experts use the term «balancing of competing interests» to describe how a more important legally protected interest takes precedence over a less important one in the event of a conflict. This principle is currently posing a dilemma for Tim Cook and Apple. As self-evident as it sounds at first, it becomes

extremely problematic when both sides claim to have the more important interest. The question of which interest is more important can be asked in the Tor case outlined above as well as in Apple's wrangle with the FBI. The media storm started even before Donald Trump called for a boycott of Apple products, and it is set to continue for some time.

Let us lay out the facts briefly. In a ruling on 16 February 2016, Judge Shery Pym ordered Apple to unlock Syed Riszwan Farook's Apple iPhone 5c. Farook and his wife killed 14 people in San Bernadino, California in December 2015. Police shot the pair dead, but the FBI wanted to investigate whether they had links to so-called Islamic State or other terrorist groups, so it requested an iOS update from Apple that would at least remove the encryption from this one smartphone.

However, Cook and Apple fear that this would set a precedent and lead to a deluge of requests. The FBI has indeed backed Apple into a corner. The case has a great deal of emotional resonance in the US, and the suspected but unproven link to terrorism increases the pressure to hack the phone from political circles, the media and the general public. The deceased attacker clearly cannot unlock the phone himself, only Apple can. The iPhone maker faces a split in public opinion. Besides Republican presidential candidate and bottle-blonde demagogue Trump, other politicians, IT giants like Bill Gates and a full 51% of people who took part in a survey rushed through by Pew Research Center U.S. Politics & Policy also think the phone should be unlocked.

Most large IT firms and politicians such as Democrat Senator Ron Wyden, on the other hand, are concerned that iPhone unlocking software could jeopardise the online security of «millions of Americans».

A growing number of reports suggest that, in addition to the FBI, other criminal investigation authorities throughout the US are asking for impounded smartphones to be unlocked in other cases. One New York district attorney alone wants over 170 iOS devices cracked.

Apple has now formally appealed against Judge Pym's ruling, which was based on the All Writs Act, a piece of legislation dating back to the 18th century. It argues that the ruling impinges on the freedom of speech guaranteed by the Constitution and that Congress has already discussed and rejected legislation for cases like this one. It is prepared to take the matter to the Supreme Court if necessary. The Cupertino-based group has gained some support from a ruling by a judge in New

York on 29 February rejecting a months-old request to unlock an iPhone in a drugs case, saying that the All Writs Act did not provide an adequate basis for a request of this nature. We have to expect that this case will drag on for a while yet.

Read more here:

http://www.faz.net/aktuell/wirtschaft/macht-im-internet/donald-trump-ruft-zum-apple-boykott-auf-14080844.html
http://www.heise.de/newsticker/meldung/US-Gericht-Apple-soll-bei-Entsperren-von-iPhone-nach-Anschlag-helfen-3107411.html
http://www.ft.com/intl/cms/s/2/3559f46e-d9c5-11e5-98fd-06d75973fe09.html#axzz41ZdlaHHP
http://www.people-press.org/2016/02/22/more-support-for-justice-department-than-for-apple-in-dispute-over-unlocking-iphone/2
http://derstandard.at/2000031344911/Donald-Trump-Was-bildet-sich-Apple-eigentlich-ein
http://www.heise.de/security/meldung/Streit-ueber-iPhone-Entsperrung-FBI-will-von-Apple-angeblich-in-weiteren-Faellen-Unterstuetzung-3115360.html
https://www.washingtonpost.com/news/post-nation/wp/2016/02/26/a-locked-iphone-may-be-the-only-thing-standing-between-police-and-this-womans-killer/?tid=sm_tw
http://www.heise.de/ct/artikel/Crypto-Wars-3-0-Hintergruende-zu-dem-Fall-Apple-vs-FBI-3116395.html
http://www.zdnet.com/article/fbi-director-iphone-unlock-case-will-be-instructive-to-other-courts/
http://www.nzz.ch/international/amerika/apple-fbi-iphone-1.18701470
http://www.nzz.ch/international/apple-muss-fbi-bei-drogenfall-nicht-beim-iphone-knacken-helfen-1.18704079

## III. Deadly bugs in hospital – ransomware Trojan Locky shuts down entire clinics and more

News of viruses in February, with more than 5,000 new infections per hour at times, had nothing to do with the flu. Instead, it was a malicious computer program that has been spreading at an alarming rate since it was first discovered. Not even hospitals or the Fraunhofer Institute in Bayreuth are safe from it. British security expert Kevin Beaumont describes the cryptolocker Locky as a «masterpiece of criminality» because it is multilingual and does not just hide in Word or Excel e-mail attachments but also spreads itself via legitimate websites as a drive-by infection (see https://www.switch.ch/saferinternet for an explanation) and can even reach drives that are not mapped to the local drive at the time of infection.

Infections disguised as JavaScript attachments and even faxes show just how broad-based the Locky onslaught is.

Its impact is especially dramatic in places where doctors and medical staff have to fight real-world viruses. In mid-February, for instance, IT systems were

completely disabled at St Luke's Hospital in Neuss, western Germany, and at least two other clinics fell victim to the cybercriminals in the state of North Rhine-Westphalia alone. Shortly afterwards, it was announced that the IT systems at the Hollywood Presbyterian Medical Center in Los Angeles had been hit by a cryptolocker on 5 February and only started working again 12 days later when the clinic transferred 40 bitcoins (about CHF 15,000) to the blackmailers via the Darknet.

Read more here:

http://www.golem.de/news/krypto-trojaner-locky-mehr-als-5-000-infektionen-pro-stunde-in-deutschland-1602-119247.html
http://www.idigitaltimes.com/new-locky-ransomware-virus-spreading-alarming-rate-can-malware-be-removed-and-files-512956
http://www.golem.de/news/ransomware-locky-kommt-jetzt-auch-ueber-javascript-1602-119331.html
http://www.heise.de/security/meldung/Neue-Virenwelle-Krypto-Trojaner-Locky-tarnt-sich-als-Fax-3117249.html
http://www.heise.de/security/meldung/Admins-aufgepasst-Krypto-Trojaner-befaellt-hunderte-Webserver-3116470.html
http://www.rp-online.de/nrw/staedte/neuss/hackerangriff-auf-lukas-krankenhaus-in-neuss-virus-noch-nicht-gebannt-aid-1.5767907
http://www.heise.de/newsticker/meldung/Ransomware-Neben-deutschen-Krankenhaeusern-auch-US-Klinik-von-Virus-lahmgelegt-3103733.html
http://hollywoodpresbyterian.com/default/assets/File/20160217%20Memo%20from%20the%20CEO%20v2.pdf

## IV. Mission: Possible – Big Data and automated law enforcement

Your own car spots when you exceed the speed limit, calculates the fine and automatically transfers it from your account to the police or, in the case of excessive speeding, turns its engine off. Although it might sound like bad science fiction at first, this kind of automated law enforcement model is not only being discussed in legal and police circles, the essential elements are already in place, albeit in rudimentary form. The latest connected cars record every movement using onboard sensors and GPS. Automated number plate recognition systems and traffic cameras are up and running not only at border crossings, but also along the motorways of many European countries – Switzerland included. Companies that rent out construction machines have been able for some time to disable their excavators, loaders and cranes remotely when a driver attempts to do overtime, be it legal or not, in excess of the working hours specified in the

rental agreement. All that is really needed to make the leap from this state of affairs to automated law enforcement is a green light from the authorities.

The Thurgau Cantonal Police have been trialling number plate scanners since 2011. At least eight more Swiss cantons are known to be scanning every vehicle on their motorways to identify those that are stolen or wanted for investigation. The data are deleted if no match is found.

Denmark is set to roll out systematic scanning and matching of all number plates at every border crossing over the course of 2016, and it plans to store the data for at least a month. Since the German and Danish police run joint patrols, data protection advocates fear that they will find a way to bypass the German ban on «recording vehicle registration numbers without sufficient grounds». Automated law enforcement is also becoming a key issue further west. Author Jonny Evans on Computerworld.com warns against connected cars because they can be hacked, force unwanted services on drivers or adversely affect warranty cover by recording their errors. Evans also notes that connected cars make the long arm of the law even longer. At the same time, he sees potential for spying by insurers to catch their customers out and use their mistakes as a reason not to pay out on claims or to increase premiums. Last but not least, Evans warns that people are handing over their data whenever they sell their car because no one knows how to delete them beforehand. John Bowman, Communications Director of the National Motorists Association, had this to say about the development of automated law enforcement technologies in the US: «If people don't push back against it…, I just think people will be surprised when they wake up one day and realise they have no privacy left.»

Read more here:

http://www.faz.net/aktuell/feuilleton/big-data-algorithmen-ermitteln-14054010.html
http://www.tagblatt.ch/nachrichten/schweiz/schweiz-sda/Polizei-scannt-Autonummern;art253650,4410588
http://www.shz.de/regionales/schleswig-holstein/politik/kennzeichen-scanner-an-grenzuebergaengen-machen-aerger-id9381871.html
http://www.computerworld.com/article/2945367/internet/just-say-no-to-connected-cars.html
http://www.autoblog.com/2014/09/23/connected-car-traffic-enforcement-featured/

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