SWITCH security report on the latest IT security and privacy trends

January/February 2020

SWITCH

I. When backdoors become trapdoors: 'Crypto Leaks' hits Switzerland, Crypto Valley – and the entire ecosystem

In its recent 'Minerva' report the CIA boasted about Operation Rubicon, describing it as 'the intelligence coup of the century'. The report was among the revelations that emerged through a joint 'Crypto Leaks' investigation conducted by *The Washington Post*, German public broadcaster ZDF, and Switzerland's Rundschau news show. The CIA report also revealed that 'Foreign governments were paying good money to the U.S. and West Germany for the privilege of having their most secret communications read by at least two (and possibly as many as five or six) foreign countries.'

For over 50 years, first through an anonymous Liechtenstein-based foundation (owned by both countries' intelligence agencies until 1992) and later Crypto AG (based in Zug and run solely by the CIA), the operation provided cipher machines and encryption/decryption algorithms with top Swiss features: precision, confidentiality, security, and neutrality. But foreign owners were getting another 'added value' that was rather less Swiss, namely a built-in backdoor to circumvent the latter three features. With trademark cynicism (see

above quote), the CIA eventually changed the code name for the operation from 'Thesaurus' to 'Rubicon', a historical reference to the events of 10 January, 49 B.C., when Julius Caesar defied the Roman Senate's orders to disband his army and cross the river unarmed. At the time, the river formed the border between the northern provinces conquered by Caesar and the frontiers of the core region of the Roman Empire, making his actions a de facto declaration of war on the Roman Senate. Ever since, 'crossing the Rubicon' has been a metaphor for crossing a red line and accepting major, even extreme risk.

And this is exactly what the CIA and BND (West Germany's and now Germany's intelligence agency) did when they fitted cipher machines with backdoors and algorithms developed in Crypto Valley to spy not only on enemy states but on allies, too. Both agencies have justified their actions by arguing that this may have prevented numerous global calamities. But the collateral damage is considerable. It is not just Switzerland as a country that is wondering what has happened to neutrality and confidentiality in the alpine republic; the Canton of Zug, which has proudly been developing and marketing its 'Crypto Valley' brand since the mid-2010s, will certainly need to reinvent itself. And crypto technologies and the crypto industry will pay dearly in the form of reputational damage.

Lack of user trust will also affect any tech company that makes its money from communication technology. After all, they have all had opportunities to include backdoors in their algorithms, enabling intelligence agencies to spy on users (which indeed proved to be the case with NSA, Cambridge Analytica and other actors, and may well still be the case – or will be again in future). The American encryption and IT specialist Bruce Schneier pointed this out in an interview with the *NZZ* (link below) and stressed that while encryption is important and useful, it does not provide complete protection: 'If a government wants to install backdoors for the purposes of espionage, it will.'

The last remaining hope is that there are some Swiss valleys too narrow for anything to slip out through a backdoor. Perhaps those will become the next, true Swiss crypto valleys.

Read more:

https://www.srf.ch/play/tv/sendung/10vor10?id=c38cc259-b5cd-4ac1-b901-e3fddd901a3d (German)
https://www.washingtonpost.com/graphics/2020/world/national-security/cia-crypto-encryption-machines-espionage/
https://www.heise.de/newsticker/meldung/Cryptoleaks-CIA-und-BND-steckten-jahrzehntelang-hinter-Verschluesselungsfirma-4658033.html (German)
https://www.nzz.ch/schweiz/der-it-spezialist-bruce-schneier-zur-crypto-affaere-ld.1540118 (German)
https://www.inside-it.ch/de/post/crypto-ag-bundesrat-veranlasst-eine-untersuchung-20200211 (German)

II. I, Robot, ZigBee and IoT

What is the difference between a robot and the Internet of Things? Robots 'understand' three simple laws designed to make them completely safe for use in the world of humans: the Three Laws of Robotics. First introduced by Isaac Asimov in his short story 'Runaround', published in 1942, the laws became a permanent feature of the plot structures in all of the books set in Asimov's universe of robotic science fiction, the first of which was *I, Robot*. The three laws:

1.) A robot may not (knowingly[3]) injure a human being or, through inaction, (knowingly[3]) allow a human being to come to harm.

2.) A robot must obey the orders given it by human beings except where such orders would conflict with the First Law.

3.) A robot must protect its own existence as long as such protection does not conflict with the First or Second Laws.

Basic security rules like these are apparently still a foreign concept when it comes to the Internet of Things (IoT). In particular, the ZigBee protocol used to link smart home devices is a continual cause for discussion. As far back as 2015, an article published for the Black Hat Conference drew attention to several security risks in ZigBee-based smart home networks. Some of the risks are even inherent to the system. To improve the security standard of these networks, the author of the Black Hat piece proposed setting up individual devices in ZigBee networks that would include anti-hacking mechanisms. Recently, a security hole was discovered in the ZigBee protocol that allowed hackers to access the networks of smart home owners using smart Philips Hue lights.

The threat potential was classified as 'high', even though any attack would require the participation of the victim, and the manufacturer has since released a security patch.

Consequently, the task of making smart home networks more secure has been making work for manufacturers and, in particular, public authorities. *heisse online* recently reported that the UK Department for Digital, Culture, Media & Sport, in cooperation with the National Cyber Centre, has devised three simple rules (a nod to Asimov) that could soon become law if passed in parliament:

1.) 'All IoT device passwords shall be unique and not resettable to any universal factory default value.'

2.) 'All companies that provide internet-connected devices and services shall provide a public point of contact as part of a vulnerability disclosure policy in order that security researchers and others are able to report issues. Disclosed vulnerabilities should be acted on in a timely manner.'

3.) ‘An end-of-life policy shall be published for end-point devices which explicitly states the minimum length of time for which a device will receive software updates and the reasons for the length of the support period.’

While this ‘Code of Practice for Consumer IoT Security’ is a bit more detailed than Asimov’s Three Laws of Robotics, it is similar in that it could serve as a main security pillar of the Internet of Things.

Read more:

https://en.wikipedia.org/wiki/Three_Laws_of_Robotics
https://www.smarthomeprofis.de/wie-sicher-ist-zigbee (German)
https://www.heise.de/security/meldung/Sicherheitspatch-Philips-Hue-Lampe-als-Sprungbrett-in-Netzwerke-4655060.html (German)
https://www.heise.de/tr/artikel/Gesetzliche-Regelungen-fuer-das-smarte-Heim-4651370.html (German)
https://www.gov.uk/government/consultations/consultation-on-regulatory-proposals-on-consumer-iot-security/outcome/government-response-to-the-regulatory-proposals-for-consumer-internet-of-things-iot-security-consultation
https://www.gov.uk/government/publications/code-of-practice-for-consumer-iot-security/code-of-practice-for-consumer-iot-security

III. Sure, it’s secure! Are you sure?

Given how much of our day-to-day lives depends on the security and integrity of digital systems, networks, hardware, and software – not to mention our exposure to threats and attacks by criminal hackers, government intelligence agencies and other dubious figures – deploying security products and systems not only makes sense but may well be essential. But of course, these types of products always increase the complexity of IT systems as well. And the more complex a system is, the more opportunities for attack it offers. In the end, the problem is similar to that of the encryption systems discussed at the beginning. They are indispensable for security but also have their own set of risks and never offer 100% protection. Symantec’s security packages are the latest example. Gaping security holes, categorised as high-risk, were discovered in the product suites Symantec Endpoint Protection (SEP), Symantec Endpoint Protection Small Business Edition (SEP SBE) and Symantec Endpoint Protection Manager (SEPM). According to Symantec, only the versions SEP and SEP SBE 14.2 RU2 MP1 (14.2.5569.2100) and SEPM 14.2 RU2 MP1 are secure. All unpatched legacy versions could potentially fall prey to DDoS attacks or even allow hackers to execute their own code on compromised devices. Symantec said that one version might even be exposed to the possibility of a DLL injection attack, and the company strongly urges users to install the latest security updates for these software packages.

Users running Fortinet’s FortiSIEM security management software up to version 5.2.6 are also vulnerable to DDoS attacks. These versions had/have a static and – to the chagrin of many – unencrypted SSH key integrated into their code. According to Fortinet, hackers could potentially extract the key in order to reconnect to the system without any additional authentication, and then carry out attacks. This is why Fortinet recommends that all of its

customers update to FortiSIEM 5.2.7 as soon as possible. Those who are not using the software's integrated reverse tunnel feature should also deactivate it (see second link for details).

Betrayed and sold to the highest bidder – that's literally what Avast did to the users of its anti-virus software when it sold its users' browser data to third-party companies on a grand scale through its subsidiary Jumpshot. The list of customers reportedly included Google, Yelp, Microsoft, McKinsey, Pepsi, Condé Nast and many more. And it had been doing this since at least October 2018, when AdBlock Plus founder Wladimir Palant discovered and revealed the data sharing. In response, Mozilla and Google blocked the installation of Avast add-ons in their browsers.

In the last Security Report, we reported that employees from the security company Trend Micro had stolen and sold the data of 68,000 customers. That pales in comparison to the Avast incident, which is in a league of its own. First, it can't be blamed on any single rogue employee. Rather, selling customer data was an integral part of the company's business model. Second, the 68,000 Trend Micro customers who were affected are small potatoes compared to the 435 million active monthly users Avast reported itself to have. Third, the sheer brazenness becomes apparent when you consider that Avast subsidiary Jumpshot boasts in its profile of being the only company that offers such valuable 'walled gardens' online and that is able to record users' complete browsing behaviour. Meanwhile, anyone who is interested in the case will discover that the website www.jumpshot.com is no longer online. Clicking on the link takes you to a page without a logo or any information – just a blank space with the text 'Jumpshot has ceased operations. Thank you.'

Read more:

https://www.heise.de/security/meldung/Sicherheitsupdates-Symantec-Endpoint-Protection-vielfaeltig-angreifbar-4659864.html (German)
https://www.heise.de/security/meldung/Fortinet-entfernt-SSH-Backdoor-aus-Security-Management-Loesung-FortiSIEM-4647473.html (German)
https://www.heise.de/newsticker/meldung/Avast-Antivirus-verkauft-massenhaft-Browser-Daten-seiner-Nutzer-4646926.html (German)
https://www.switch.ch/export/sites/default/security/.galleries/files/security-reports/SWITCH-Security-Report-2019-06-de.pdf
https://www.prnewswire.com/news-releases/jumpshot-strikes-strategic-partnership-deal-with-ascential-to-provide-marketers-with-deeper-visibility-into-the-entire-online-customer-journey-300888439.html?tc=eml_cleartime

IV. A different kind of virus: China launches its Close Contact Detector app for smartphones

When we report on viruses in our Security Report, normally we are referring to digital viruses that infect and compromise all kinds of devices. Now we are reporting on a medical virus for the first time, because attempts by the Chinese government to control the spread of the SARS-CoV-2 virus – more commonly referred to as the 'coronavirus' – have demonstrated the subtlety and all-encompassing nature of the surveillance apparatus in

the world's most populous country. On 11 February, the BBC reported that in response to the evidently pandemic spread of confirmed coronavirus infections, the Chinese government had launched an app to warn users when they come into contact with people who are confirmed or suspected to be infected. The app is downloaded using a QR code reader, such as the ones integrated in the payment app Alipay or on the social media platform WeChat. The app registers (and sends) the number of the smartphone on which the app has been installed. The user then has to enter their name and ID number and will subsequently receive notifications when they are at risk of infection, in which case they are asked to stay at home and notify the local health authorities.

The functioning of the app appears to rely on data of confirmed or suspected virus carriers combined with the data and movement profiles of the app user. What makes it so efficient is clearly a dense surveillance network, the prime example and most elaborate instance of which is found in the 'Xinjiang Uygur Autonomous Region'. BuzzFeed has described it as 'what a 21st century police state really looks like'. The communication platform persoenlich.com added: 'In the battle to curb the spread of SARS-CoV-2, China is ramping up its full arsenal of surveillance technology'. And this raises several questions: Is this an act of strategic planning to stop the spread of the coronavirus as effectively as possible? Is it a case of panicked desperation by an overwhelmed government? Is it a totalitarian regime's sheer cynicism – or perhaps something in between? Even if it was launched with the best of intentions, there are fears that the new app will give conspiracy theorists even more fodder – as if they need it.

Read more:

https://www.bbc.com/news/technology-51439401
https://futurezone.at/netzpolitik/app-warnt-wenn-man-kontakt-mit-coronavirus-infizierten-hatte/400751361 (German)
https://9to5mac.com/2020/02/11/coronavirus-app
https://www.engadget.com/2020/02/12/china-close-contact-detection-app-coronavirus
https://www.buzzfeednews.com/article/meghara/the-police-state-of-the-future-is-already-here
https://www.persoenlich.com/digital/china-kampft-mit-daten-gegen-virus
https://www.engadget.com/2018/02/22/china-xinjiang-surveillance-tech-spread
https://insideparadeplatz.ch/2020/01/29/stammt-corona-virus-aus-wuhan-waffenlabor (German)

This SWITCH security report was written by Dieter Brecheis and Frank Herberg.