SWITCHcert Security Report

January 2016

I. Does PrivaTegrity spell the end of crypto wars? David Chaum's new encryption system bridges gap between completely anonymous communication and crime prevention

David Chaum is seen as the father of anonymity and privacy on the Internet. In the «crypto wars» between companies, governments and criminal prosecutors on one side and defenders of radical, unrestricted freedom and absolute anonymity on the other, Chaum has developed various encryption systems and programs that practically underpin Internet anonymity as we know it today. He has now come up with an new communication network, unveiled at Stanford University's Real World Crypto conference, that aims to end the crypto wars by establishing a kind of truce between the two opposing camps: «You have to perfect the traceability of the evil people and the untraceability of the honest people.»

With this in mind, PrivaTegrity is designed to allow users to communicate with total anonymity. Chaum claims that it cannot be cracked by intelligence services or hackers, making it safer than the Tor network, for example. Even though the core of PrivaTegrity, high-performance scalable mixing, runs on nine servers plus a «management» server separated from the nine and from the transferred codes (compared with three volunteer machines for Tor), it should allow communication via a smartphone app and be at least as fast as Tor. Chaum and his team are initially developing the network for Android.

PrivaTegrity has a back door built in to ensure that it does not become a safe haven for terrorists and criminals, but this is not accessible to government departments. Instead, the nine server administrators are to form a «Backdoor Security Council» that decides when to strip users of their anonymity based on their communications indicating criminal or terrorist activity. The intention is therefore for most of the PrivaTegrity servers to be located outside the US in countries with legitimate democratic governments. The examples Chaum gives are Canada, Iceland and Switzerland.

Read more here:

http://www.wired.com/2016/01/david-chaum-father-of-online-anonymity-plan-to-end-the-crypto-wars
http://www.gulli.com/news/26982-verschluesselungssystem-privategrity-soll-komplett-anonyme-kommunikation-bieten-2016-01-11
https://www.hackread.com/new-anonymous-communication-network-privategrity-launched
https://de.wikipedia.org/wiki/David_Chaum
https://de.wikipedia.org/wiki/Crypto_Wars

II. The boss is listening, and it's OK – controlled surveillance of private communications at work does not violate human rights

The European Court of Human Rights (ECHR) passed a judgment with far-reaching implications at the start of this year. It said that employers who monitor their staff's work computers and smartphones do not violate their staff's privacy or human rights, even where personal or intimate communications are concerned, provided they observe certain strict rules. According to the ECHR judgment, employers have to ensure that their staff fulfil their contractual duties during working hours, and they have the right to check that this is the case. Article 8 of the European Convention on Human Rights, which provided the legal basis for creating the ECHR, comprehensively protects employees' privacy. Employers must therefore operate reasonable and well founded monitoring based on a policy and rules for the use of e-mail and messaging services that have been clearly defined in advance, and they must inform their staff about this.

The judges ruled that these conditions had been met in this case. A Romanian engineer had brought the case before the court because he was sacked after his employer accused him of failing to fulfil his duties in view of his extensive personal use of chat services, providing 45 pages of chat records as evidence of this. The judges ruled in favour of the employer. This judgment is particularly timely as staff chats are becoming increasingly popular. It is binding for all signatory states of the European Convention on Human Rights, including Switzerland.

Read more here:

http://www.handelsblatt.com/finanzen/steuern-recht/recht/europa-urteil-arbeitgeber-duerfen-chatprotokolle-ausspaehen/12834104.html
http://www.humanrights.ch/de/menschenrechte-schweiz/inneres/person/datenschutz/schutz-privatsphaere-arbeitsplatz
http://www.bbc.com/news/technology-35301148
http://www.mittelstand-die-macher.de/recht-finanzen/it-internetrecht/urteil-chatten-am-arbeitsplatz-ist-ein-kuendigungsgrund-19865
http://www.karriere.at/blog/buerokommunikation.html

III. Yesterday's science fiction, today's reality – forecasting software and systems to spot crimes before they are committed

Agatha, Arthur and Dashiell possess drug-induced powers that allow them to predict future murders, complete with the names of the perpetrators. They help the Washington police department's «Precrime» unit to keep the murder rate in the US capital at zero for six years running. This is the plot of 2002 science fiction thriller «Minority Report», based on a short story with the same name from 1956 written by Philip K. Dick, who also provided the inspiration for «Blade Runner» and «Total Recall». Exactly 60 years after Dick's story, police in the German cities of Karlsruhe and Stuttgart – both in the state of Baden-Württemberg – are working with the Precrime Observation System or Precobs. Police in the state of Bavaria and the Swiss cantons of Zurich, Basel-Landschaft and Aargau are also using the software, primarily to predict break-ins. The thinking behind this is the «near repeat» theory, according to which crimes are more likely to occur in places where crimes have already been committed. The software attempts to extrapolate patterns from information on the circumstances and timing of crimes, tools used and so on. It then uses these patterns to calculate probabilities for future crimes. This is of course a million miles from the film's portrayal of drug-induced visions and immersive networking with personal data from other sources, including iris recognition for the entire population. However, data protection advocates warn that linking it up with social media profiles, criminal records and other data sources, such as movement patterns from connected driving profiles and i-beacons (all of which are depicted in «Minority Report»), could ultimately lead to blanket surveillance and, in the worst-case scenario, innocent people being accused of crimes. Indeed, these digital cops do not exactly have a perfect record of success so far. Police in the UK county of Kent, who were among the pioneers of «predictive policing», actually reported an increase in the crime rate after their system was introduced.

A working group of the Internet Engineering Task Force has made its own reference to classic science fiction. In a nod to Ray Bradbury's novel «Fahrenheit 451», they created the HTTP status code 451 Unavailable For Legal Reasons. This is intended to show users more clearly than 400 Bad Request, 403 Forbidden and 404 Not Found why a requested Internet resource is blocked.

Code 451 should be especially frequent (or perhaps entirely absent) in China, where the government has blocked over 6,000 domains and countless search terms for years with its «Great Firewall» in order to maintain its sovereignty even over the Internet.

Read more here:

http://www.nzz.ch/international/deutschland-und-oesterreich/kommissar-kristallkugel-1.18667054
http://www.tagesanzeiger.ch/zuerich/stadt/Minority-Report-in-Zuerich/story/12692897
http://orf.at/stories/2261957/2261958
https://bigdatablog.de/2015/08/03/predictive-policing-big-data-in-der-polizeiarbeit
http://www.theguardian.com/cities/2014/jun/25/predicting-crime-lapd-los-angeles-police-data-analysis-algorithm-minority-report
http://www.bbc.com/news/uk-england-kent-32529731
http://www.zeit.de/digital/internet/2015-12/fehlermeldung-451-statuscode-zensur
http://www.theregister.co.uk/2015/12/21/censorship_451_error_code_approved_by_ietf
http://www.nzz.ch/international/asien-und-pazifik/ein-schutzwall-gegen-westliches-gedankengut-1.18666754
http://www.nytimes.com/2015/08/18/opinion/murong-xuecun-scaling-chinas-great-firewall.html?_r=0
http://www.faz.net/aktuell/wirtschaft/fruehaufsteher/zensur-im-internet-china-zieht-die-great-firewall-hoeher-13386343.html

IV. A patchy start to the year – reports of security issues read like a who's who of network equipment suppliers

The year began with unwelcome news of security loopholes and back doors for Juniper Networks, Fortinet, Cisco, AVM and UPC, not to mention their customers. Juniper Networks, for example, had to field questions as to why it had waited so long to remove the random number generator Dual_EC_DRGB from the ScreenOS operating system used by its NetScreen firewalls. It has been known for years that Dual_EC has a back door for the US National Security Agency, and other clues point to the UK intelligence centre GCHQ. Juniper has also declined to explain why it was using Dual_EC in the first place, given its reputation for slow speed and poor quality.

Fortinet has faced similar criticism after security researchers discovered that older versions of its FortiOS firewall operating system grant full administrator rights to anyone using Secure Shell access with a fixed password. The company did say that this was not a back door and that it had already released a patch in mid-July 2014, but the risk of attacks on all FortiOS versions from 4.3.0 up to and including 5.0.7 is nevertheless rated as high.

Another network equipment supplier, Cisco, found no less than four security issues rated high to critical in its hardware and software products. While it claims that no attacks have been recorded to date, the company is advising its customers to download the latest security updates as soon as possible. One critical issue concerns the Identity Services Engine (ISE) version 1.1 or later, 1.2.0 before Patch 17, 1.2.1 before Patch 8, 1.3 before Patch 5 and 1.4 before Patch 4. Another concerns Cisco's 2500, 5500 and 8500 Series wireless controllers running its Wireless LAN Controller (WLC) software from versions 7.6.120.0, 8.0 and 8.1. A threat Cisco rates as high, meanwhile, concerns the Aironet 1830e, 1830i, 1850e and 1850i access points, which require a firmware update. A second vulnerability in the ISE, affecting version 2.0 and older, is rated as medium but should nevertheless be closed without delay. Cisco is also continuing to warn users about the security issues with OpenSSL that were published in December. A list of the devices affected can be found at the link below beginning «tools.cisco...».

There is also bad news for Fritzbox users: models 3272/7272, 3370/3390/3490, 7312/7412, 7320/7330 (SL), 736x (SL) and 7490 running firmware older than version 6.30 have vulnerabilities that allow hackers to make phone calls at the Fritzbox owner's expense, intercept data transferred via the router and attack devices connected to the local network. Manufacturer AVM has released a firmware update that it urgently recommends installing.

UPC has also published a security recommendation for its routers after the UPC Recovery Tool was published on Twitter. The tool makes it possible to discover the default Wi-Fi passwords of UPC home routers and thus hack them.

It looks like this new year is set to bring plenty more work for security experts.

Read more here:

http://www.computerworld.ch/news/security/artikel/juniper-firewalls-muessen-gepatcht-werden-69351
http://www.heise.de/security/meldung/Juniper-entfernt-NSA-Zufallsgenerator-aus-Netzwerkgeraete-Betriebssystem-3067616.html
http://www.heise.de/newsticker/meldung/Festeingestelltes-Wartungs-Passwort-gefaehrdet-Fortinet-Appliances-3069680.html
http://www.darknet.org.uk/2016/01/fortinet-ssh-backdoor-found-firewalls
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20151204-openssl
http://www.heise.de/security/meldung/AVM-Router-Fritzbox-Luecke-erlaubt-Telefonate-auf-fremde-Kosten-3065588.html
http://avm.de/ratgeber/sicherheit/tipps-fuer-zusaetzliche-sicherheit/uebersicht-fritzbox-modelle-und-sicherheitsupdate

The Clipboard: interesting presentations, articles and videos

The Data Protection Commissioner for the Canton of Zurich now has a YouTube channel and has already uploaded an awareness video:

https://www.youtube.com/channel/UCghVVLU_hOTbClYaKQk8hTw

In addition, the Commissioner's website features a data protection tutorial:

https://review.datenschutz.ch/datenschutz/index.php?jss=1

159 videos of talks given at this year's Chaos Communication Congress (32C3) are online:

https://media.ccc.de/c/32c3

Please tell us what you think in our reader survey!

SWITCH is conducting a reader survey for the Security Report and would be grateful if you could share your views on how we can improve it. Your help will allow us to tailor the Security Report better to your needs and make it even more appealing. All of the information you provide will be analysed in anonymised form.

Please complete the questionnaire by Friday, 31 January 2016 at the latest. It will take you roughly 8-10 minutes.

The links below take you straight to the questionnaire:
German: http://swit.ch/befragung-secrep
English: http://swit.ch/survey-secrep

Please do not hesitate to contact us if you have any questions about the survey: roland.eugster@switch.ch.
Thank you very much for your help.

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