SWITCHcert Security Report

June 2014

SWITCH

I. Heartbleed is not over yet

Swift action was needed at the start of April. A serious vulnerability was found in the ubiquitous OpenSSL software library that had the potential to expose passwords and SSL keys. It was labelled an Internet disaster. System administrators all over the world were called on to respond as quickly as possible by applying the available patches and replacing keys.

Now that the dust has settled, it is worth taking another look at the situation, since not everything has gone well. Investigations by various security researchers have revealed that

- about 7% of systems that were patched and given a new SSL certificate are still using the old key.
- Thousands of administrators appear to have updated OpenSSL, but from an older version not affected by Heartbleed to one that is not secure, thus introducing Heartbleed to their servers for the first time.
- At least a quarter of the affected servers are yet to be fixed a month after the problem was disclosed.

While most system administrators reacted quickly and intelligently, this means that it is still too soon to give the all-clear.

There is also another reason for this: Attention has so far been focused mainly on web servers, but OpenSSL is used in many other places as well, and these are no less critical. They range from servers for e-mail, video, phone and other services to firewalls, VPN nodes and industrial plant control systems.

Research is now being conducted into new attack vectors. Security researcher Luis Grangeia, for example, is looking into the possibility of exploiting Heartbleed via wireless authentication (EAP) in order to attack WLAN clients. He recently told Threatpost.com, «This vulnerability has the potential to give attackers an open door to corporate networks.»

Read more here:

http://news.netcraft.com/archives/2014/05/09/keys-left-unchanged-in-many-heartbleed-replacement-certificates.html

http://blog.erratasec.com/2014/05/300k-servers-vulnerable-to-heartbleed.html

http://www.csoonline.com/article/2154240/data-protection/research-gives-reason-to-double-check-heartbleed-fix.html

http://www.theregister.co.uk/2014/05/09/unpatched_failboxes_see_thousands_join_heartbleed_club/

http://threatpost.com/heartbleed-exploitable-over-enterprise-wireless-networks/106422

II. One year on, still no end to NSA scandal

A year after Edward Snowden's first leaks, the situation is sobering. The NSA, GCHQ and almost all the world's spy agencies are continuing with their unchecked mass surveillance and data-gathering in spite of all the criticism levelled against them.
In May, the publication of further NSA documents backed up suspicions that the NSA's Tailored Access Operations (TAO) group intercepts hardware sent by post in order to install spyware known as «beacon implants». William Binney, who resigned from his post as NSA Technical Leader in 2001, had already publicised the fact that the NSA can access servers, routers and other network devices manipulated in this way.

The New York Times reported at the start of June that the NSA has been harvesting photos across all communication channels in a targeted manner since 2011. Millions of images, said the paper, are filtered daily using the Tundra Freeze facial recognition program, and around 55,000 a day are usable. According to an internal NSA paper,

this process is intended to identify and track not only terrorists, but also other «intelligence targets».
There are grounds to fear that this may include Swiss banks, especially since Snowden's confidant Glenn Greenwald told *Tagesanzeiger* in an interview that there was evidence of the NSA spying on the Swiss banking system.

It seems only logical, therefore, that people at Swiss and Swiss-based research institutions should be working on new Internet and security standards. The ETH Network Security Group is developing a new Internet architecture with much greater security. The SCION project's aims include enabling senders and recipients to steer the routing of their data themselves so as to avoid pathways that are vulnerable to interception. Meanwhile, three scientists from CERN have created a start-up and launched a new anti-spying e-mail service called ProtonMail. The strict separation of authentication and decryption, the obligatory use of two passwords to log in and mail servers located exclusively in Switzerland make ProtonMail NSA-proof, its developers say.

Read more here:

http://www.heise.de/newsticker/meldung/NSA-manipuliert-per-Post-versandte-US-Netzwerktechnik-2187858.html

http://blogs.cisco.com/news/internet-security-necessary-for-global-technology-economy

http://www.nytimes.com/2014/06/01/us/nsa-collecting-millions-of-faces-from-web-images.html?_r=0

http://www.netsec.ethz.ch/research/SCION

http://home.web.cern.ch/about/updates/2014/05/cern-inspires-entrepreneurs-email-encryption

III. The Internet learns how to forget

A few days ago, Google started providing a web form that allows European customers to request the removal of some search results containing their name. This is the search engine giant's response to a judgement by the EU Court of Justice on 13 May guaranteeing individuals a «right to be forgotten» on the Internet under certain circumstances.
The judgement states that any request to this effect must be addressed directly to the search engine operator, which must then «duly examine its merits». Where the operator does not grant a request, the individual concerned may bring the matter before the relevant data protection authority or the courts.

Federal Data Protection and Information Commissioner Hanspeter Thür sees this judgement as a «bold decision». He told *Tagesanzeiger*, «It's a good day for data protection. For the first time, it's been acknowledged that search engines process data and are thus subject to the law on data protection. This represents a massive improvement in the legal situation for the individuals concerned.»

However, not all sides are taking an equally positive view of the Court's acknowledgement that «a fair balance between the legitimate interest of Internet users and the data subject's fundamental rights» must be sought. Handelsblatt.de quotes Ole Schröder, Secretary of State in Germany's Ministry of the Interior: «We have to prevent search engines from arbitrarily deleting opinions and information.» The German Journalists Association has expressed alarm: «Freedom of information must be accorded the same importance as data protection,» said GJA National Chairman Michael Konken. The German ICT industry association BITKOM is also critical of the judgement. It claims that a case-by-case assessment weighing up the right to privacy against freedom of information is not practicable for search engine operators.

No one has yet provided details of the extent to which Google's procedure actually works. There are rumours that Google has already received thousands of deletion requests. A copy of a valid photo ID must be uploaded with each request for authentication purposes. Legal expert Thomas Stadler claims that this procedure is problematic, at least in Germany: «The ID can be used as (electronic) proof of identity, but it must not be stored by Google. Whenever a file is uploaded, it is automatically stored somewhere,» he writes in his blog.
In addition, it remains to be seen how other search engine operators such as Microsoft and Yahoo respond to the ruling.

Read more here:

http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-05/cp140070de.pdf

https://support.google.com/legal/contact/lr_eudpa?product=websearch

http://www.tagesanzeiger.ch/schweiz/standard/Ein-guter-Tag-fuer-den-Datenschutz/story/11314698

http://www.golem.de/news/nach-eugh-urteil-google-schlichtungsstelle-soll-recht-auf-vergessen-regeln-1405-106768.html

http://www.nzz.ch/aktuell/digital/google-setzt-recht-auf-vergessenwerden-um-1.18312335

http://www.bitkom.org/de/presse/8477_79340.aspx
http://www.internet-law.de/2014/05/google-stellt-formular-fuer-antrag-auf-entfernung-aus-den-suchergebnissen-gemaess-europaeischem-datenschutzrecht-online.html

The Clipboard: Interesting presentations, articles and videos

SSL certificate fuzzing – US researchers have developed a method for finding bugs in SSL libraries using randomly mutated and bundled certificates:

http://www.heise.de/security/artikel/SSL-Fuzzing-mit-Frankencerts-2166135.html

Network security firm FireEye has broken down its Advanced Threat Report 2013 for Europe. Switzerland comes in second place in terms of the percentage of unique infections by country. In the statistics for unique infections by industry vertical, higher education features very prominently in fourth place:

http://www.fireeye.com/blog/corporate/2014/04/the-fireeye-advanced-threat-report-2013-european-edition.html

At this year's Troopers14 security conference, Enno Rey discussed the fundamental difficulties with IPv6 security. His talk and 26 others from the conference are available online:

http://www.youtube.com/channel/UCPY5aUREHmbD04PtR6AYLfQ

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