Editorial

Mobile danger: Precautionary Measures : Android

Erroneous safety updates on the mobile apparatus can draw along with it in future penalty money and damage compensation (indemnity).

In March 2018 the new global centre for cyber safety with its seat in Geneva was to have opened which was to be executed by World Economic Forum (WEF). In its up-to-date global risk report the WEF warned urgently against the danger through cyber attacks. These were in this year the unique top catastrophic scenario which had gone out neither the environment nor the climate change. Alone in the last five years, the number of the attacks increased to twofold.

Cyber safety belongs to the most urgent themes of our time – said WEF director Mr. Alois Zwinggi. With the new centre he now wants to bring the governments of G20 states and international organizations to a table in order to initiate a dialog on the theme. The development of new technology such as artificial intelligent, robotics drone's automatic vehicles or the internet of things (IoT) depends on an urgent safe environment according to WEF.

Sudden attack of the WEF received detonating violence through the most recent cyber super GAU meltdown and specter on the chip level which fall upon almost all computers and mobile phones. The attackers can make the best use of the safety gaps in the hardware architecture of many processor chips and therefore read out all data as also passwords and entry codes which are processed in storage battery. Along with Intel and AMD also processors on the basis of ARM architecture are affected. These are obstructed in many smart phones and tablets. Only few chips are not affected.

The hardware safety gaps require updates in all management systems applications and activities, emphasizes the safety researcher Daniel Gruss of Gratz against VDI nachrichten. Gruss described with his colleagues on the attack scenario of meltdown and spectre. From that place the security GAU still for a long time not overcome.

As problem child in mobile domain market leader android is in operation. The mobile management system is developed by open handset Alliance to the consortium. In the meantime 84 times belong to the consortium. It was set up by Google Android is based on Lynx and is a free software whose original text lies open.

Today android, the leading smart phone management system has worldwide business coverage of 88%.

Therefore android is for the damaged software developer importantly more active than Apples iOS, Security researcher Christoph Meinel of Hasso-Plattner-Institute (HPI) says so. The wide expansion of android system makes the software as the object of attack specially attractive for the criminals. Simultaneously the experts nevertheless search extensively also for gaps. Correspondingly many weak places are found there.

First since 2015 Google prepares the safety updates for android which are then delivered directly only to the Google instrument of the production series Pixel and Nexus. Alone 28 securities updates for the search machine giant lastly at android patch paid in February 2018 to mobile management system. With that however only instruments of android versions 5.1.1. and

higher are supplied (provided). Old versions of the management system remain without update. Google informs the manufacturers of android instruments one month before standing in a queue updates which they then can take up out of the android open source project.

Generally the instrument manufacturers themselves decide whether and how long they can deliver security updates. Only a fraction of the instrument is therefore taken care of from the really at the disposal remaining security updates. So at present only the users of Blackberry, LG, Samsung and top models of few other manufacturers receive monthly safety patches, by which also here few instruments are consequently taken care of afterwards.

It is additionally problematic that android through updating and expanding always become more complex and with that susceptible to defect. HPI researcher Meinel recommends therefore:

- User should be cautious that their instruments from manufacturers to cover up regularly to execute the update.

Google controls the android distributions lastly on through that Google applications like e-mail or the play store only of android versions are permitted to be used which the Google has licensed. On that Google has also the possibility to erase or to install on the Apps installed on the instrument per distant attack without the cooperation of the users.

Unlicensed android versions do not exhibit these safety functions. Before all the Chinese instrument manufacturers use unlicensed Android versions which they partly develop further in their own operation system. Google services are namely blocked in china and the purchasers on the play store are not permitted. Also Amazon uses for its kindle fire instrument, the Fire OS, the one further own development of Android.

In view of this unsatisfactory situation there are however two expectation gleams for the users. To one, the new European data safety basic directive however guarantee already from May 2018 from the firms, IT safety as per "Stand of Technique". The manufacturers could not mislead the compensation to more activity but also users could namely additionally accuse the firms on the damage substitute for immaterial damages whereby customers not as before but the firms are bound for the proof of evidence. To the other set-ups as the new "global centre for cyber safety" are therefore instituted that the firms take care of the security gaps and manage customer friendly relation.

HPI (Hasso-Plattner-Institute) offers safety checks.

- Under https://hpi-vdb.de – The users can compile a list of their up-to-date programme versions which is then by the HPI service permanently on the security gaps checked. In total about 96000 weak spots are stored in the HPI databank for IT attack analysis which falls upon around 224000 programmes and 17000 manufacturers.
- The databank collects all important nearby available published in internet particulars on security gaps and security problems. The gradation of weak grades of weak places occur on the basis of free open and strongly utilized industrial standards CVSS (Common Vulnerability Scoring System).

Source: FOKUS: mobile Gefahr, VDI nachrichten, 23 Februar, Nr. 8

Anil Kumar Ghosh
Editor-in-Chief,
Indian Science Cruiser