Systemic Errors as Vulnerabilities

DeepSec and Privacy Week highlight consequences of backdoors in IT

Ever since the first messages were sent, people try to intercept them. Today, our modern communication society writes more small, digital notes than one can read along. Everything is protected with methods of mathematics - encryption is omnipresent on the Internet. The state of security technology is the so-called end-to-end encryption, where only the communication partners have access to the conversation content or messages. Third parties can not read along, regardless of the situation. The introduction of this technology has led to a battle between security researchers, privacy advocates and investigators.

Kick down Doors with Horses

In end-to-end encryption the keys to the messages, as well as the content itself, remain on the terminal devices involved in the conversation. This is the desired goal, because this type of communication uses networks that are not trustworthy or public, such as the Internet. There is no other way to communicate securely in these environments. End-to-end encryption is without alternative. This is also proven by history. Legislation requiring communications service providers to grant government agencies access to users' communications led to the development of Pretty Good Privacy (PGP) software in the 1990s. The clashes at the time therefore bear the name Crypto Wars in the English-speaking world.

One meets the hurdles of mathematics with ancient means. Backdoors or Trojan horses, ie embedded software for reading messages before encryption, should be used directly on terminals in order to be able to read along at the source. In terms of security, however, backdoors represent a weak point in hardware or software. For the use of Trojan horses, a vulnerability must be present in order to be able to surreptitiously install the application. Both approaches are diametrically opposed to information security.

Built-in Abuse

Even if authorities should use the so-called state trojans only for the investigation of drug offenses or similar serious cases, it’s conceivable that such an interception software escapes and is put to another purpose. The wiretapping affair in Greece in 2004 is a real example. At that time, telephone calls and messages from Greek government and government officials were recorded via the lawful interception interfaces in the mobile network. The attackers exploited the existing interfaces. Kostas Tsalikidis, the mobile operator's network planning manager, was found dead in his home two days after the security gap was revealed. The perpetrators of the monitoring scandal were never found despite years of investigation.

Although, in software, no built-in interfaces for monitoring are active per se or provided for, there are prerequisites that must be fulfilled. With a state trojan, sometimes called a federal trojan, the state actively exploits vulnerabilities in computer programs or apps in smartphones to monitor individuals. Often the state itself even buys these weaknesses on the black market with taxpayers' money and deliberately does not inform the development companies about the vulnerabilities it then knows about, in order to keep the security gaps open as long as possible for its own purposes. In doing so the security of all people and computer systems is put at risk. At a meeting in August 2018, the Department of Cyber Security and IT Security of the Federal Ministry of the Interior confirmed that the knowledge of unknown security vulnerabilities has been held back to a certain extent and not made public in order to attack digital systems.

Close Gaps instead of exploiting them

From the very start the DeepSec security conference has been dealing with security issues. In recent years, the security of mobile networks, Internet infrastructure, mobile devices, all kinds of applications, software components of operating systems and much more has been analyzed in detail. Vulnerabilities are not suitable as a foundation on which to build a house safely. Security researchers worldwide agree that only the publication of mistakes (in collaboration with interested manufacturers) leads to their correction. In times of discussion about campaign manipulation, threats to critical infrastructures, increasing networking in sensitive industries and military use of software, the highest possible level of information security is more important than ever. Therefore, the DeepSec conference again will feature presentations and trainings on this topic in November of this year. Especially recommended are the lectures, which specifically deal with the perpetrators. Edith Huber and Bettina Pospisil will present the results of their research on profiles of perpetrators and victims of cybercrime. Dr. Silke Holtmanns will discuss the state of the art in terms of security in mobile networks in her lecture, as well as the challenges for 5G. Mark Baenziger will take the tensions between supervisors and supervised as an opportunity to illuminate the activities in an IT security team from both points of view.

Lectures on the Topic at Privacy Week

There are two lectures on the subject of State Trojans at PrivacyWeek. In his presentation, Andre Meister, longtime editor at netzpolitik.org, gives an overview of the state of the art used in state trojans, the laws, which allegedly regulate them and the numerous problems in their implementation. His presentation bears the title of the topic - "State Trojan". Lukas Gahleitner of Amnesty International Austria gives a lecture entitled "The Protective Duties of States regarding Human Rights, or What do marine mines off the Albanian coast have to do with the state Trojan horse?", which will illustrate the international legal dimension of the topic. Ultimately, vulnerabilities are a threat to a states own infrastructure and citizens. So what should be done if a state knows about vulnerabilities? In this regard Lukas Gahleitner has suggestions to make and puts them up for discussion.

Program and Booking

The DeepSec conference takes place on the 29th and 30th of November.
The trainings take place on the two previous days, the 27th and 28th of November.
Training & Conference venue: The Imperial Riding School Vienna - A Renaissance Hotel, Ungargasse 60, 1030 Vienna.
You can find the current program under the link: https://deepsec.net/schedule.html
Tickets for the DeepSec conference and trainings can be ordered via the link https://deepsec.net/register.html.

The Privacy Week will take place from the 22nd to the 28th of October 2018 at the Folklore Museum in the 8th district of Vienna.
The program can be found at https://fahrplan.privacyweek.at/.
The tickets for the Privacy Week can be ordered online via https://privacyweek.at/tickets/.