Intelligence Agencies want to abolish Information Security

DeepSec conference criticizes the open attack on secure end-to-end encryption

Ever since security measures have been in existence, there have been discussions about their benefits and their strength. In digital communication, the topic of back doors keeps coming up. In the analog world high quality locks are desired to protect against theft. In the digital world this may now change. The Five Eyes (i.e. the intelligence services of the United States, the United Kingdom, Australia, New Zealand, and Canada) want to force all countries around the world to implement duplicate keys, thus to implement back doors, in their encrypted communication. For this purpose, at the end of August, a meeting of the Five Eyes Ministers of the Interior took place in Australia. This proposal has serious disadvantages for the economy and national security of each state.

Messenger instead of Mobile Radio

As the mobile phones began their triumph, there were only unencrypted short messages (also known as SMS, Short Message Service). Before the era of smartphones, some manufacturers have developed their own proprietary formats to protect the content of messages. In recent years, there has been a shift towards messenger apps that use the Internet for messaging. Thus developers could and can use open standards with strong encryption, which are not subjected to the legally prescribed interfaces for telecommunication monitoring in the mobile radio networks. This telecommunication surveillance (also internationally called Lawful Interception) is an integral part of the network infrastructure and constantly records location data, logins, operating hours, addresses, mobile radio identifications and other data. Modern messengers therefore usually use the principle of end-to-end encryption, where only the communicating terminals have the keys to the message. The network does not know these keys and can not see the content of the messages. This is only possible via mobile data access, ie Internet access.

The dangers of the interfaces of mobile radio networks have been illustrated by the published documents of Edward Snowden in 2013 and the Greek wiretapping scandal (also known at the Athens Affair) in 2004 and 2005. As early as 2015, James Bamford, an American journalist and intelligence expert, gave the opening speech of the DeepSec conference, explaining how the Greek government's mobile phones were being tapped by strangers via legally required backdoors. Kostas Tsalikidis, the responsible network officer, committed suicide days after the monitoring configurations became known. The perpetrators of the wiretapping campaign were never traced, despite the most lengthy investigations.

In Australia Mathematics is not legally binding

Security researchers and engineers are well aware of the dangers of poorly implemented and insecure communications. For this reason, at the latest since the Snowden revelations, strong cryptography and secure communication are pushed ahead by technology companies and developers. The Institute of Electrical and Electronics Engineers (IEEE) and the Internet Engineering Task Force (IETF) have standardized protocols in all standards of recent years that contain neither backdoors nor deliberately weakened algorithms. The modern Internet, and thus our present communication society, is based on these standards. The technicians are trying to create the counterpart to safe bridges, which must also have no predetermined breaking point. Infrastructure must be reliable. One must not forget that not only telephone calls and messages are affected by the legal weaknesses. Demands for key escrow concern financial transactions, the complete World Wide Web, all applications on smartphones, the Internet of Things, all smart technologies, in short, all companies and markets worldwide.

Former Australian Prime Minister Malcolm Turnbull has given the highest priority to the demands of the enabling to read all communications worldwide, everywhere. In July this year he stated that the Australian Code of Law is above mathematics. He referred to the criticism of researchers in cryptography, which is a branch of mathematics. This logic is questionable, because no one has previously declared gravity to be illegal in order to prevent accidents at work or to climb mountains more easily. The only question is whether you want real security or not. Fire protection is a good analogy. No one wants protection against fires that do not always work. Likewise, nobody wants to use electronic means of payment, which are only safe until further notice.

National security is abolished internationally

The demand of the Five Eyes can also be rephrased. Since their services also use mathematics to protect their countries, they would have to weaken themselves. This would particularly concern industrial espionage, which often crosses national borders. Complete destruction or sabotage of important information security components is a short-sighted reflex. It's not just about the flagship companies of Silicon Valley. Backdoors and duplicate keys endanger all communications, from trade secrets to the secure electronic communication of lawyers with the judiciary and public authorities.

It should not be forgotten that this demand will not only be made by the Five Eyes, should it be implemented by governments. The United Nations currently has a list of 206 member states. The demands of the Five Eyes will then be requested by the "206 Eyes". Political leaders are very well advised not to ignore the warnings of experts. If one agrees with the demand for backdoors, the Five Eyes must then also reveal their own national (secret) communication to Europe, Russia, China and North Korea, to put it bluntly. This has nothing to do with reality, and certainly not with information security.

There are no Solutions within a Monologue

Security researchers are in the same boat as the authorities. They too have to find attackers and have to work with or against protective measures. However, IEEE, IETF and all technical organizations are not reluctant to demand strong security. Since the demands of the Five Eyes explicitly call for legislative action, this is a high compliment to the technicians, cause this means that the technical implementation is very difficult to attack, or not assailable by means currently available.

The implementation of security is always the result of interdisciplinary cooperation. That's why the DeepSec conference aims to bring together representatives from research, government, business and the international hacker community every year. A networked world needs networked thinking. Isolated solutions or short-term measures are not promising. Therefore, this year's DeepSec conference focuses on infrastructure, the Internet of Things, mobility (be it wireless/radio, device or transport), and cryptography. Specialists from four continents will meet to exchange ideas in Vienna in November to counter the threats of the future. We look forward to constructive cooperation and your visit.

Sources, Schedule, 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

James Bamford has summarized his talk in the publication “In-Depth Security - Proceedings of the DeepSec Conferences Volume 2” as an article entitled "A Death in Athens - The Inherent Vulnerability of Lawful Intercept. " The book is available in stores and via the DeepSec conference (it can be ordered directly from DeepSec GmbH).
His talk can be viewed online at https://vimeo.com/150691584.

Tickets for the conference and trainings can be ordered via the link
https://deepsec.net/register.html.